Alaotsikko: INCLOUD: FLAVORIN MUUTOS (RESIZE INSTANCE)

VALMISTELUT

Instanssin flavorin muutokseen kannattaa varata 30-60 minuuttia, jonka aikana instanssista muodostetaan Snapshot ja flavor muuttuu valitsemaasi flavoriin.

Suosittelemme myös ottamaan Snapshotin sammutetusta instanssista ennen toimenpiteitä, jotta palautus ongelmatilanteessa on helppoa.

Lisätietoa eri flavoreista löytyy INcloud 9 hinnastosta ja Ominaisuudet-sivulta.

HUOMIOT

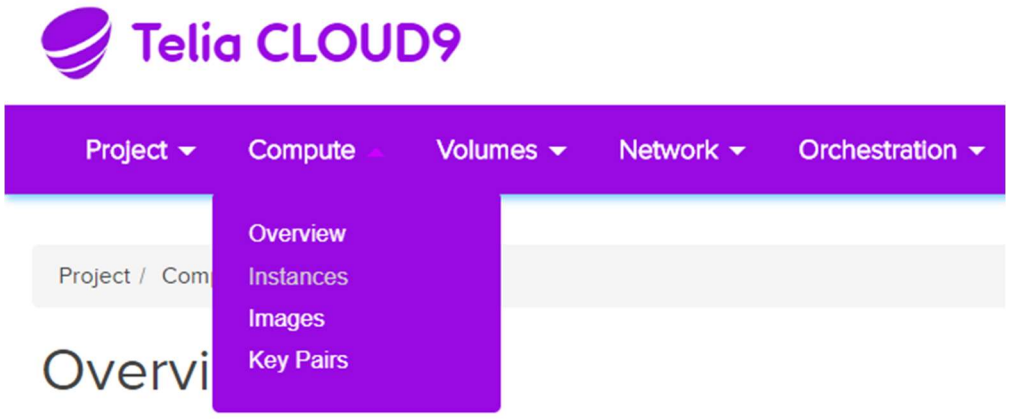
- Instanssi tulee sammuttaa (mieluiten käyttöjärjestelmätasolta) ennen operaatiota.
- Flavorin muutoksessa ei ole mahdollista valita flavoria, jossa on pienempi juurilevy kuin nykyisessä koossa.
- Huomiothan mahdolliset Prepaid-tilaukset ennen muutoksien tekemistä.
  Olemassa olevien Prepaid-tilauksien tulisi täsmätä käytössä olevia flavoreita tai muuten instanssi laskutetaan On-Demand hinnaston mukaisesti flavorin muutoksen jälkeen.

VAIHEET

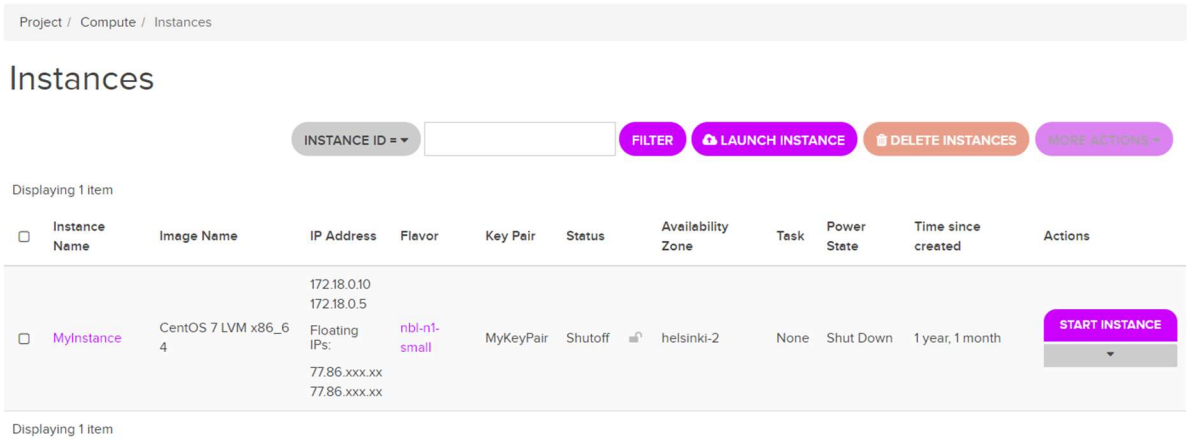
Tässä esimerkissä instanssista otetaan snapshot ja se kasvatetaan flavorista *NBL-N1-SMALL* isompaan *NBL-N1-MEDIUM* flavoriin.

1. Kirjaudu pilvenhallinnan päänäkymään. (https://control.nebulacloud.fi)

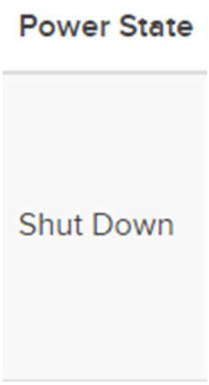
2. Avaa instanssilista ylävalikon kautta. (**Compute -> Instances**)



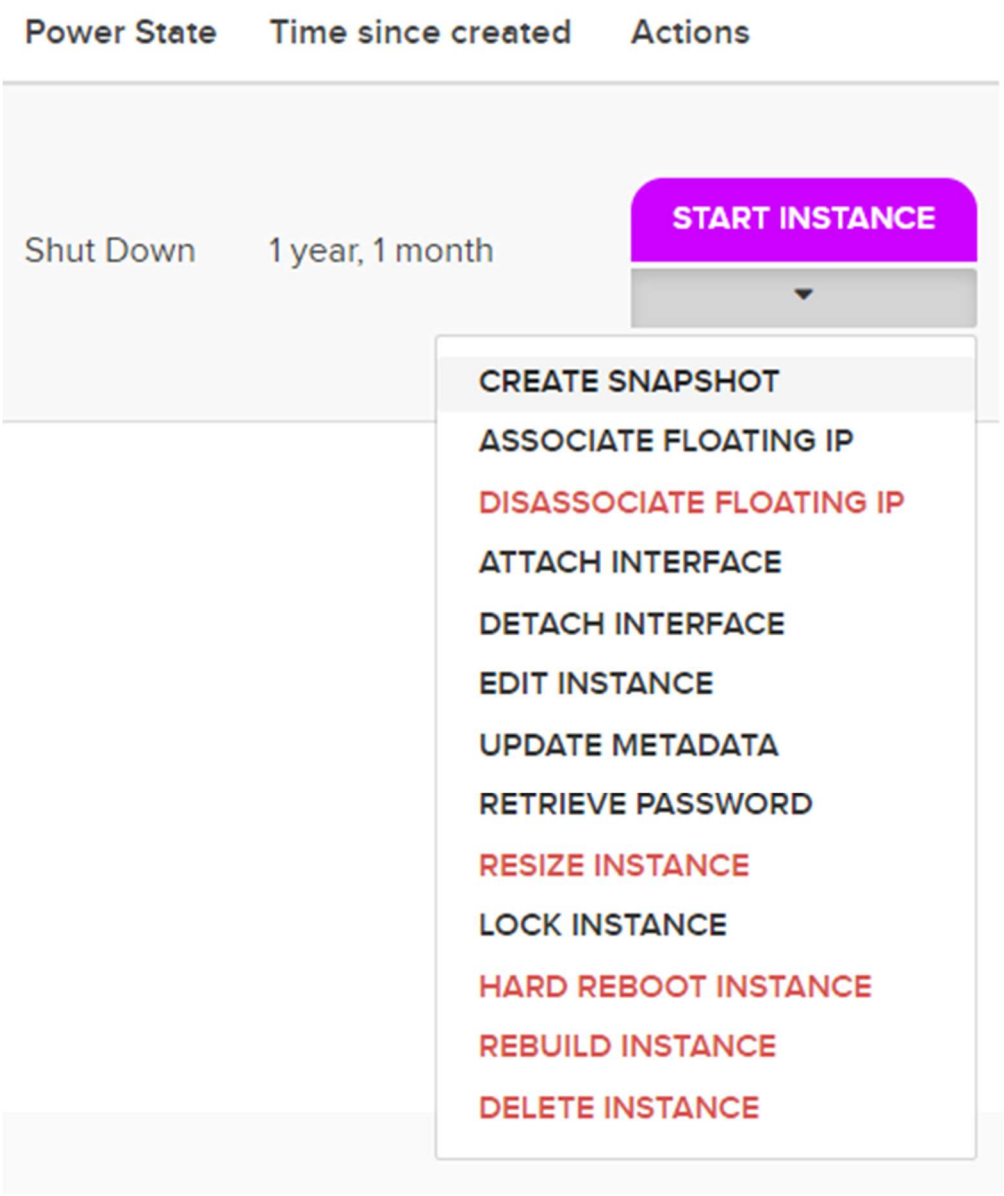
3. Etsi listasta haluamasi instanssi, jolle on tarkoitus tehdä flavorin muutos.



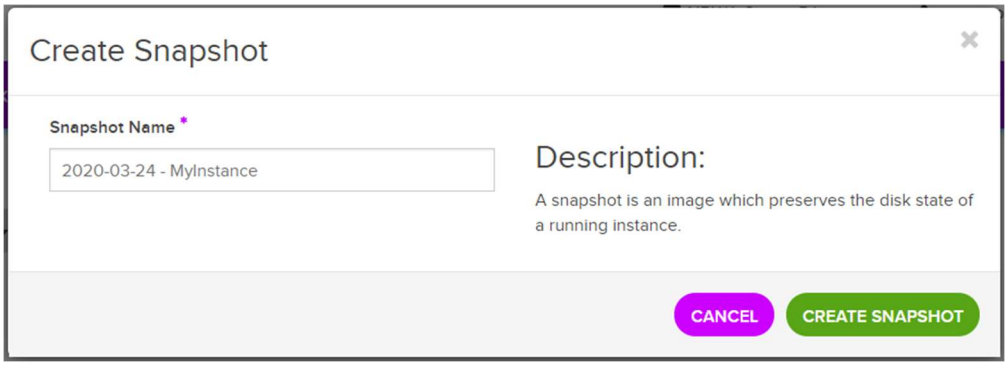
4. Varmista, että instanssi on sammunut. (**Power State = Shut Down**)



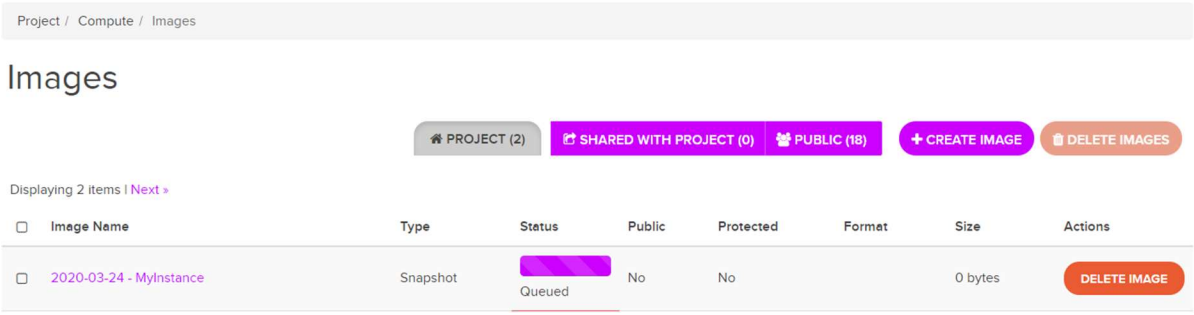
5. Ota instanssista Snapshot. (**Actions -> Create Snapshot**)



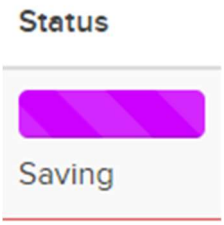
6. Valitse uudelle Snapshotille jokin nimi ja klikkaa “**Create Snapshot**“.



7. Seuraavaksi alusta alkaa muodostamaan Snapshottia.
Tämä kestää tyypillisesti 15-60 minuuttia riippuen juurilevyn koosta.

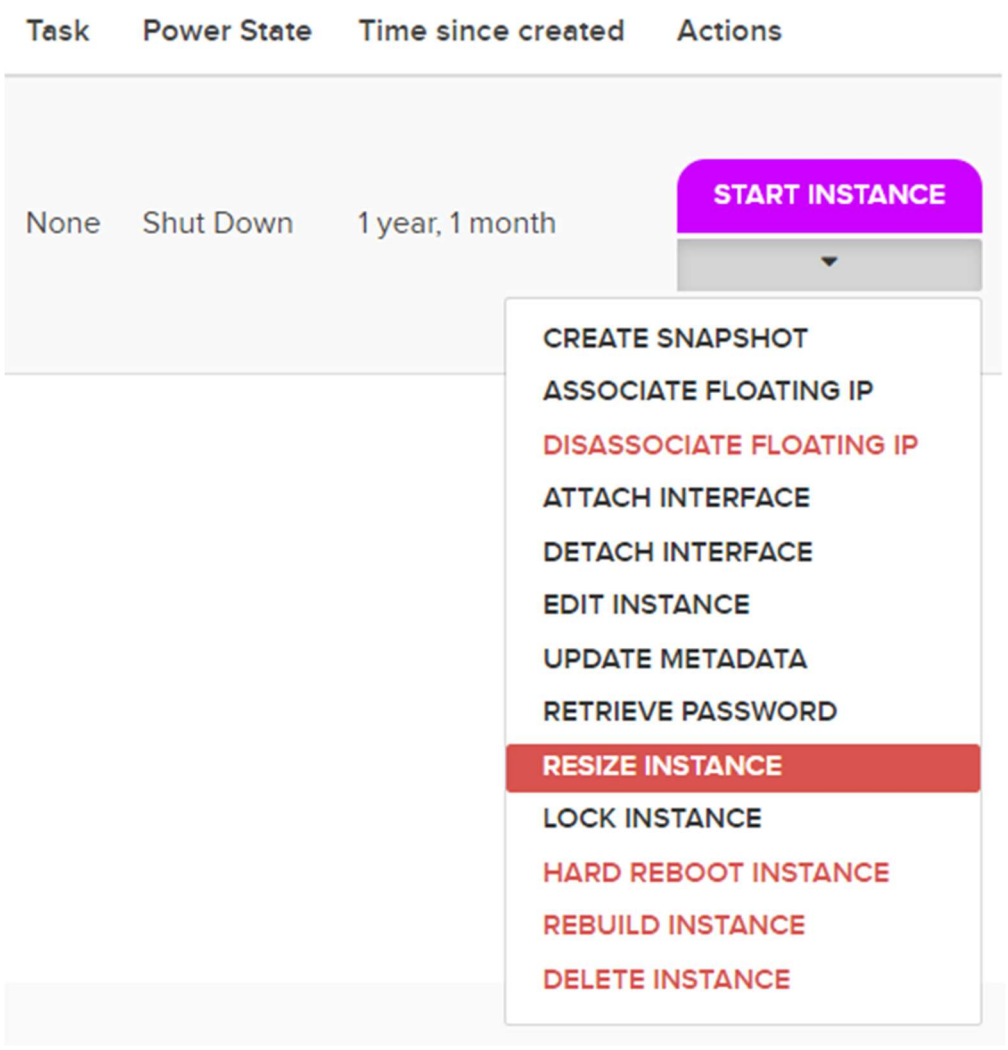


8. Hetken kuluttua Snapshotin tila muuttuu **Saving**-tilaan.

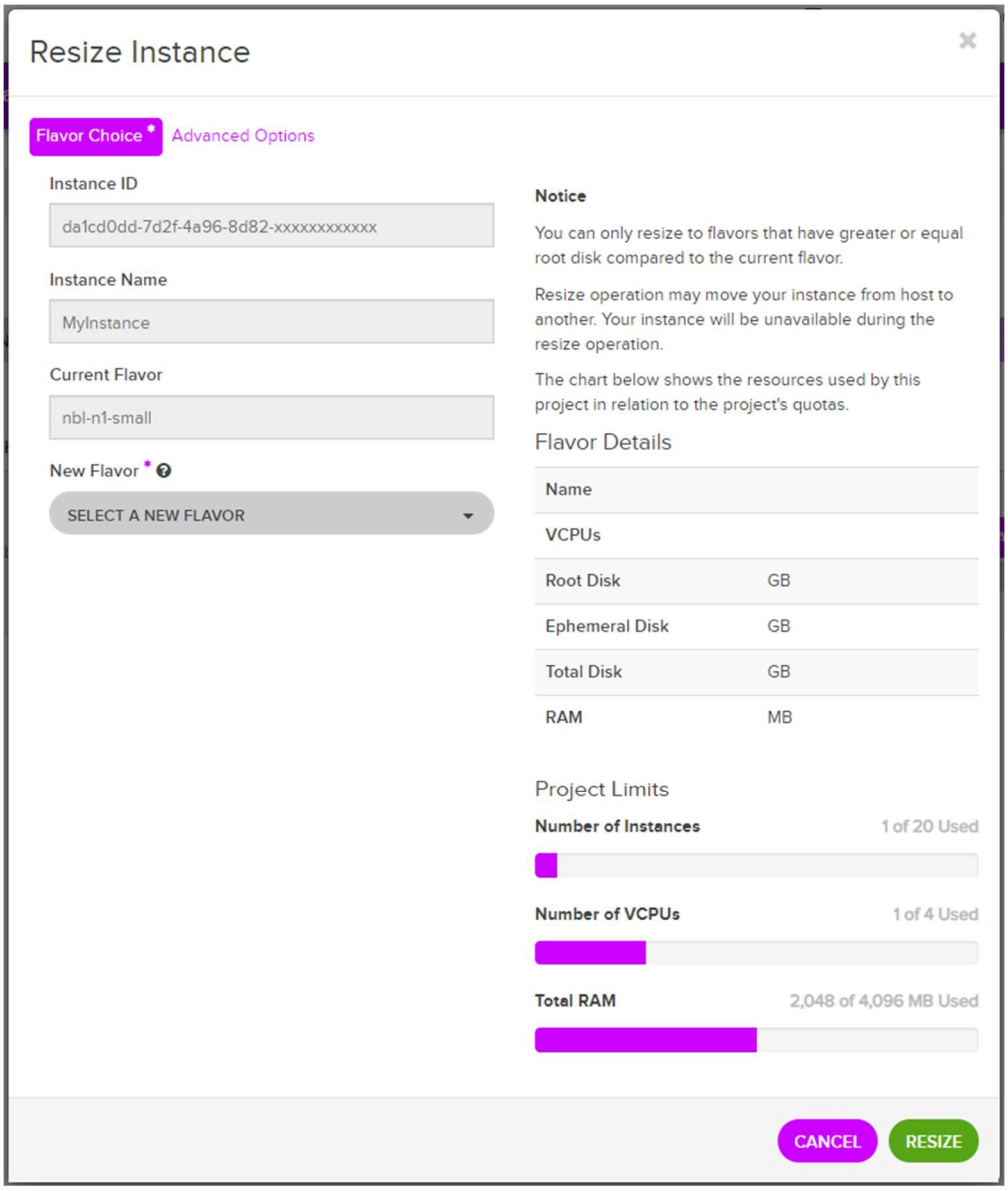


9. Snapshot menee **Active**-tilaan, kun se on valmistunut.

10. Palaa takaisin instanssilistaan ja valitse instanssin kohdalta “**Resize Instance**“. (**Actions -> Resize Instance**)

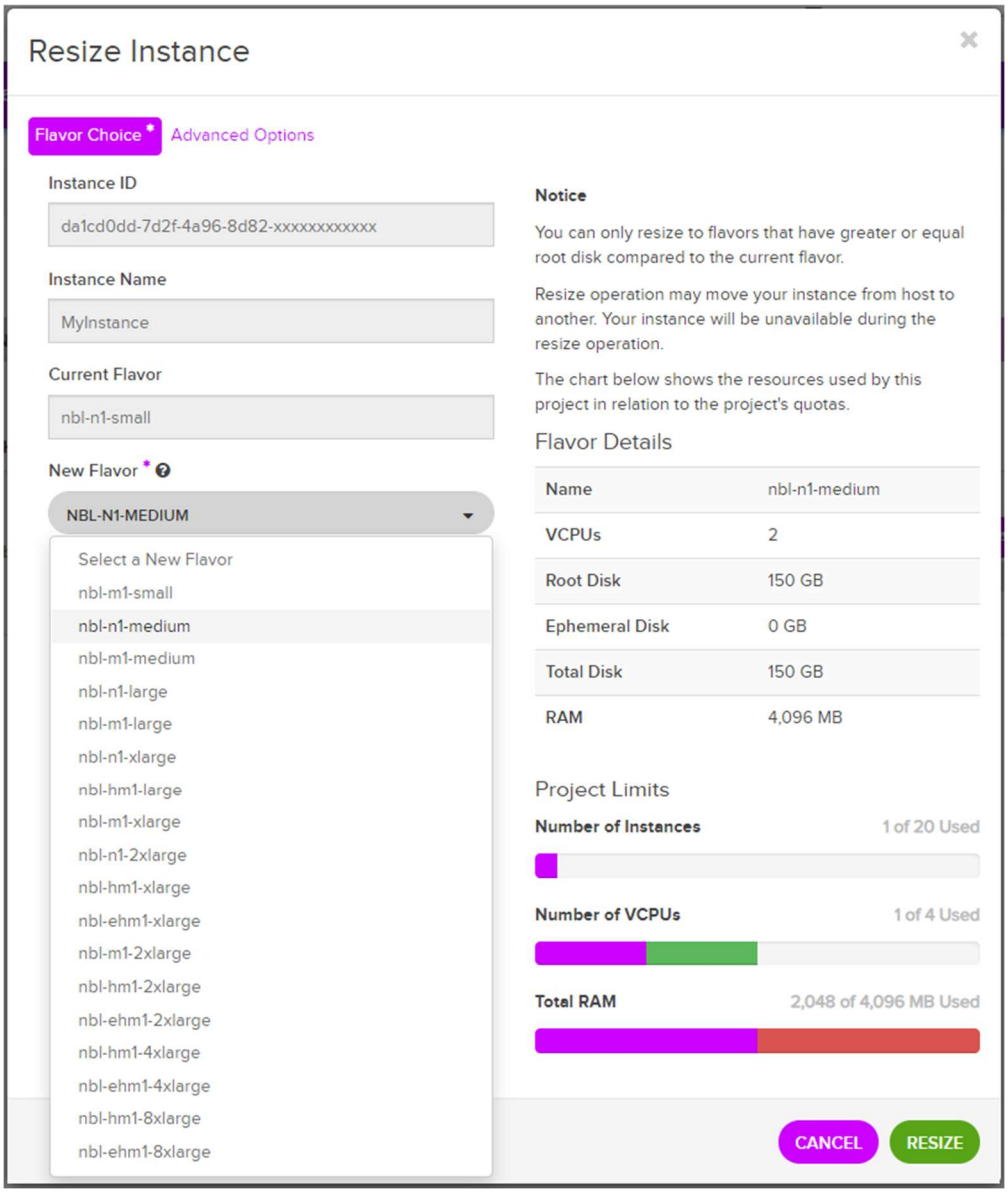

Task
Power State
Time since created
Actions
None
Shut Down
1 year, 1 month
START INSTANCE
CREATE SNAPSHOT
ASSOCIATE FLOATING IP
DISASSOCIATE FLOATING IP
ATTACH INTERFACE
DETACH INTERFACE
EDIT INSTANCE
UPDATE METADATA
RETRIEVE PASSWORD
RESIZE INSTANCE
LOCK INSTANCE
HARD REBOOT INSTANCE
REBUILD INSTANCE
DELETE INSTANCE

11. Valitse Resize Instance -lomakkeesta kohde flavor. (**Flavor Choice -> New Flavor**)

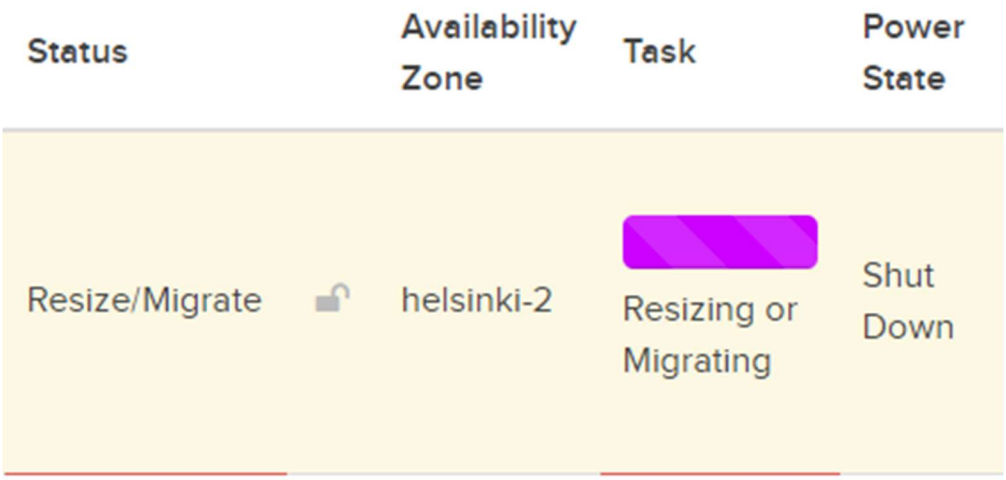


12. Tässä esimerkissä valitaan kohde flavoriksi *NBL-N1-MEDIUM*.
Tämä tuo instanssille lisää yhden virtuaalisuorittimen ja kaksi gigatavua muistia.

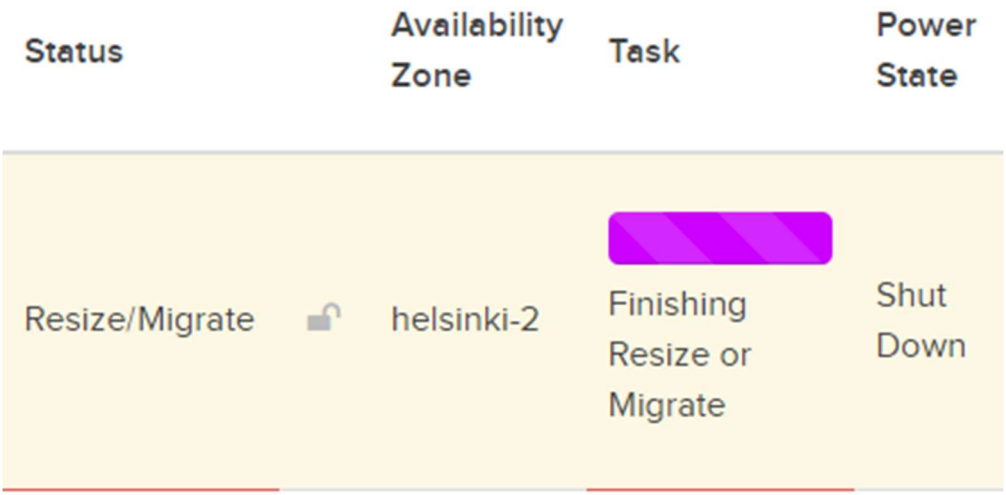
Mikäli projektisi Quota eli rajoituksen tulevat tässä kohdassa vastaan, olethan yhteydessä asiakastukeemme rajoituksen nostamiseksi.
Kerrothan yhteydenotossasi projektin nimen (tai ID:n) ja tarvittavan kapasiteetin.



13. Valittuasi halutun kohde flavorin, klikkaa **Resize**.
Palaudut instanssilistaan hetken kuluttua, jossa näet instanssin “**Resizing or Migrating**” tilassa.
Operaatio kestää tyypillisesti 15-30 minuuttia riippuen flavoreista.

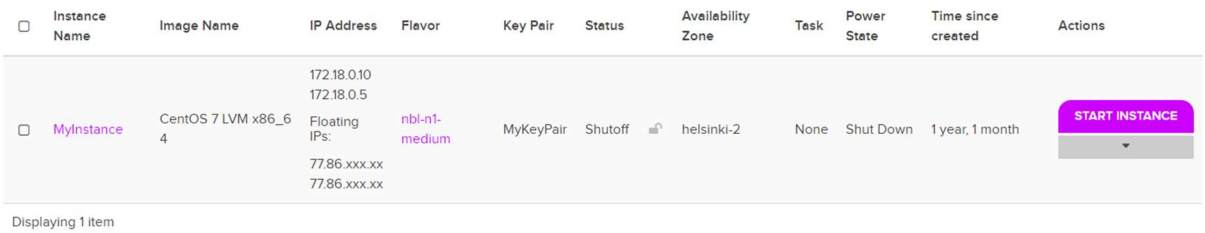


14. Näkymään tulee "**Finishing Resize or Migrate**", kun operaatio on lähes valmis.



Pienen hetken jälkeen muutos tulee vielä vahvistaa klikkaamalla "**Confirm Resize/Migrate**".

15. Hetken kuluttua instanssi palautuu **Active**-tilaan ja **Flavor**-sarakkeessa näkyy uusi valittu flavor. Tässä vaiheessa voit käynnistää instanssin klikkaamalla "**Start Instance**".



VIIMEISTELY

Instanssin flavorin muutos ei välttämättä muuta esimerkiksi juurilevyn osioiden kokoa. Tämä vaihtelee käyttöjärjestelmästä ja Image-tyypistä riippuen, joten perehdythän käyttämäsi käyttöjärjestelmän dokumentaatioon.

Mikäli instanssi toimii normaalisti, voi aiemmin otetun Snapshotin poistaa. (**Compute -> Images -> [aiemmin luotu Snapshot] -> Actions -> Delete Image**)

Alaotsikko: INCLOUD: INSTANSSIN KÄYNNISTÄMINEN LEVYKUVASTA

Joissain tilanteissa on tarpeen korjata asennettua instanssia (virtuaalipalvelinta) käynnistämällä se levykuvasta (ISO-image), esimerkiksi tilanteessa jossa Windows hajoaa päivitysten johdosta eikä käynnisty enää. Tämä onnistuu siirtämällä korjaukseen käytettävä levykuva palveluun, ja tämän jälkeen käynnistämällä instanssi rescue-tilaan halutusta levykuvasta.

Palvelimen voi käynnistää rescue-tilassa myös valmiiksi palvelussa olemassa olevilla levykuvilla, eli samoilla joilla uusi instanssi provisioidaan, mutta tällöin instanssi käynnistyy väliaikaisesti nk. “uutena asennuksena” ja instanssin alkuperäinen juurilevy näkyy toisena levynä käyttöjärjestelmälle. Instanssin palautus rescue-tilasta normaaliksi käynnistää palvelimen jälleen alkuperäisellä juurilevyllään. Tämä ei ole aina toimiva tapa korjata instanssia, joskus esimerkiksi Windowsin asennusimagen (“CD-image”) käyttö korjauksessa on toimivampi ratkaisu.

Tämä ohje käsittelee oman levykuvan (ISO-image) siirtoa palveluun, ja instanssin käynnistämistä siirretyltä levyimagelta rescue-tilaan. Ohjeessa käytetään hyväksi OpenStackin komentorivityökalua, eikä kaikki ohjeessa mainitut toimenpiteet välttämättä onnistu web-käyttöliittymän kautta.

LEVYKUVAN SIIRTO PALVELUUN OMALTA TYÖASEMALTA

Levykuvan siirto palveluun OpenStackin komentorivityökalulla onnistuu seuraavasti, esimerkissä on käytetty työasemalta palveluun siirrettävää “*systemrescuecd-amd64-6.1.0.iso*“-levykuvaa jota halutaan käyttää instanssin korjaukseen. Levykuvan nimen voi valita itse – esimerkissä se on “*systemrescuecd*“.

openstack image create --file systemrescuecd-amd64-6.1.0.iso --disk-format iso --container-format bare --min-ram 768 --property hw_cdrom_bus=scsi systemrescuecd

INSTANSSIN KÄYNNISTYS RESCUE-TILAAN LEVYKUVASTA

Kun levykuva on siirretty palveluun aiemman kohdan mukaisesti vaadituilla lisäattribuuteilla, onnistuu instanssin käynnistys rescue-tilaan seuraavasti käyttämällä image-attribuuttina aiemmassa kohdassa siirtämäsi imagen nimeä (esimerkissä "*systemrescuecd*") ja viimeisenä attribuuttina korjattavan instanssin UUIDtä (uniikki ID). Instanssin UUIDn saa selville esimerkiksi listaamalla kaikki projektin instanssit komennolla "*openstack server list*".

openstack server rescue --image systemrescuecd e6567abc-c041-4de4-f656-a50850bc802d

Kun halutut toimenpiteet instanssille on tehty, onnistuu sen käynnistys alkuperäisellä juurilevyllään palauttamalla instanssi normaalitilaan:

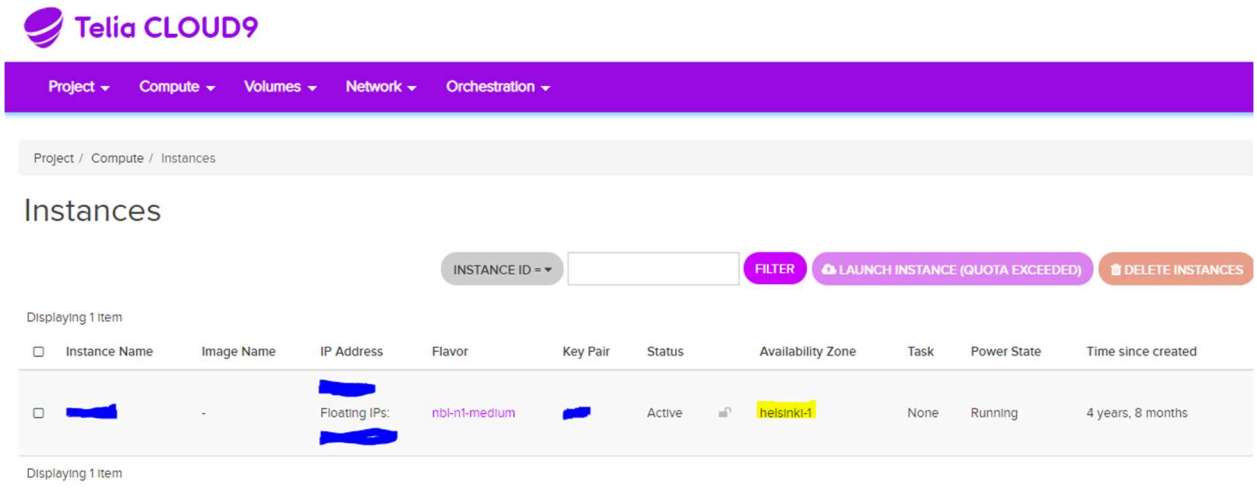
openstack server unrescue e6567abc-c041-4de4-f656-a50850bc802d

Unrescue-komennon jälkeen instanssi käynnistyy automaattisesti uudelleen aluperäiseltä levyltään.

Alaotsikko: INCLOUD: INSTANSSIN SAATAVUUSALUEEN TARKISTAMINEN

Tämän ohjeen avulla voit tarkistaa, millä saatavuusalueella Cloud 9 -instanssisi sijaitsee.

1. Kirjaudu ensin hallintapaneeliin osoitteessa https://control.nebulacloud.fi
2. Navigoi valikkoon Compute > Instances
3. Instanssin saatavuusalue on ilmaistu "Availability Zone" -sarakkeessa



Alaotsikko: INCLOUD: LEVYKUVAN SIIRTÄMINEN INCLOUD 9-PALVELUUN

Voit siirtää halutessasi työasemaltasi löytyvän levykuvan INcloud9-palveluun ja provisioida siitä uuden instanssin.

Korkeintaan 4096MB kokoisen levykuvan siirtäminen INcloud 9-palveluun onnistuu verkkoselaimella Horizon-hallintapaneelin (control.nebulacloud.fi) kautta, mutta ensisijaisesti suositeltu tapa levykuvien siirtämiseen on käyttää OpenStackin Glance-levykuvapalvelun komentorivityökalua (linkki työkalun dokumentaatioon). Komentorivityökalua käyttäessä palveluun siirrettävälle levykuvalle ei ole aiemmin mainittua kokorajoitusta, eli se koskee vain selaimella tehtäviä siirtoja.

Kunhan Glance-työkalun toiminnan vaatimat palvelun kirjautumiseen käytettävät ympäristömuuttujat on asetettu oikein ja autentikointi onnistuu, voi levykuvan siirtää palveluun komentorivityökalulla seuraavasti:

glance image-create --name "Uusi_levykuva" --file "levykuvan_paikallinen_tiedostonimi.qcow2" --progress

Name-valinta määrittelee uuden levykuvan nimen INcloud 9-palvelussa, file-valinta määrittää siirrettävän levykuvan sijainnin työasemalla jolta levykuvaa ollaan siirtämässä, ja progress-valinta näyttää siirron tilaa sen aikana.

Tietoa muista komentorivityökalun argumenteista levykuvan luonnin yhteydessä löytyy työkalun omasta dokumentaatiosta.

Esimerkki Novan komentorivityökalun asennukseen Windows-työasemalle löytyy täältä. Sama Novan ohje pätee myös levykuvapalvelun työkaluun sillä erolla, että Glancen komentorivityökalun paketin nimi on *python-glanceclient*.

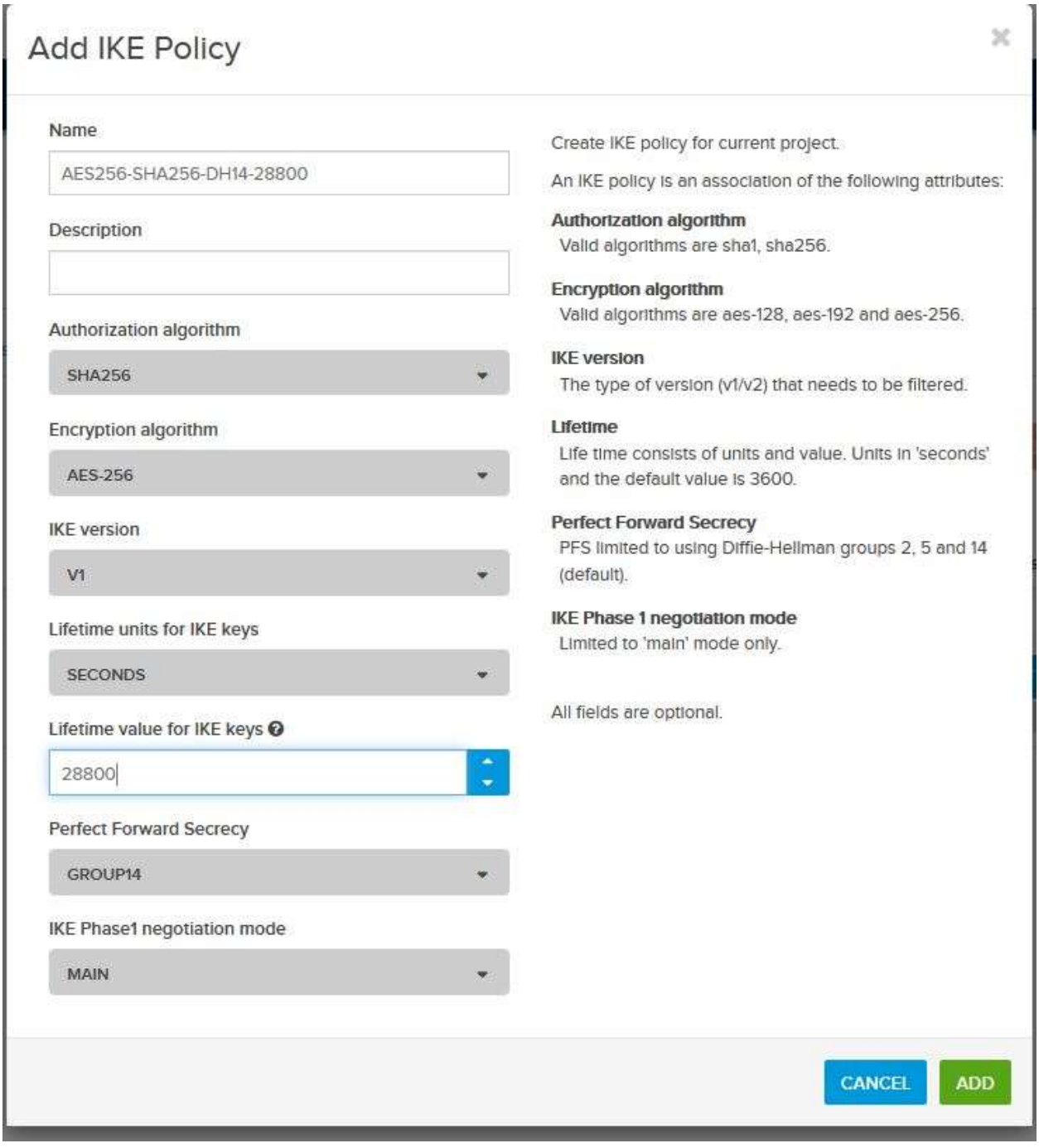
Alaotsikko: INCLOUD: VPNAAS-YHTEYDEN MUODOSTAMINEN

Ennen VPN-tunnelin tekoa INCloud 9- ympäristössä tulee olla luotuna Network/Subnet, johon palvelimet ovat kytkettyinä sekä Router, johon Network/Subnet on liitetty.

Valitse ylävalikosta: **Network-> VPN**

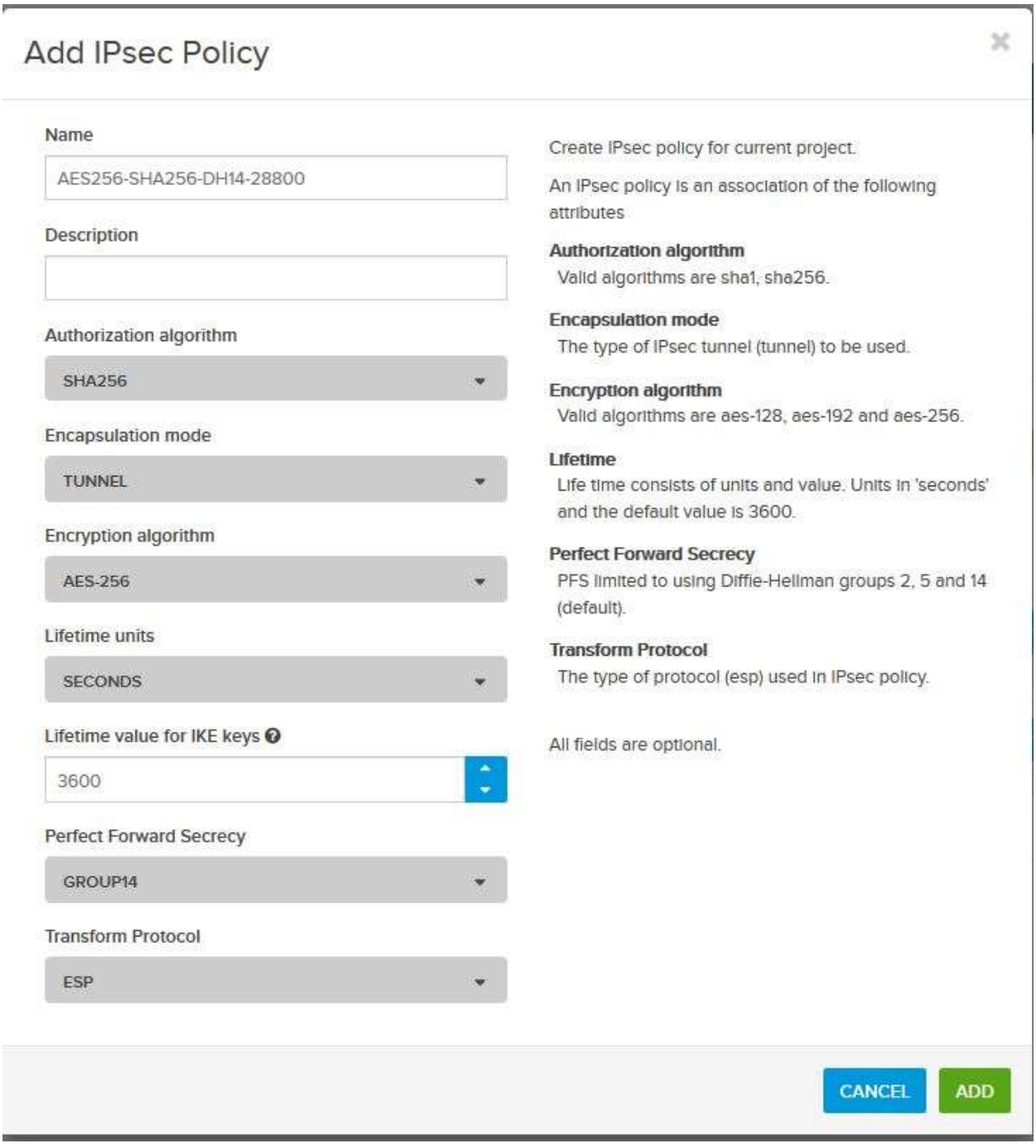
Valitse IKE Policies -välilehti ja lisää uusi Policy: **+ ADD IKE POLICY**

Lisää IKE Policyyn kuvaava nimi ja salaukseen halutut parametrit alasvetovalikoista sekä hyväksy policy **ADD** -painikkeella.



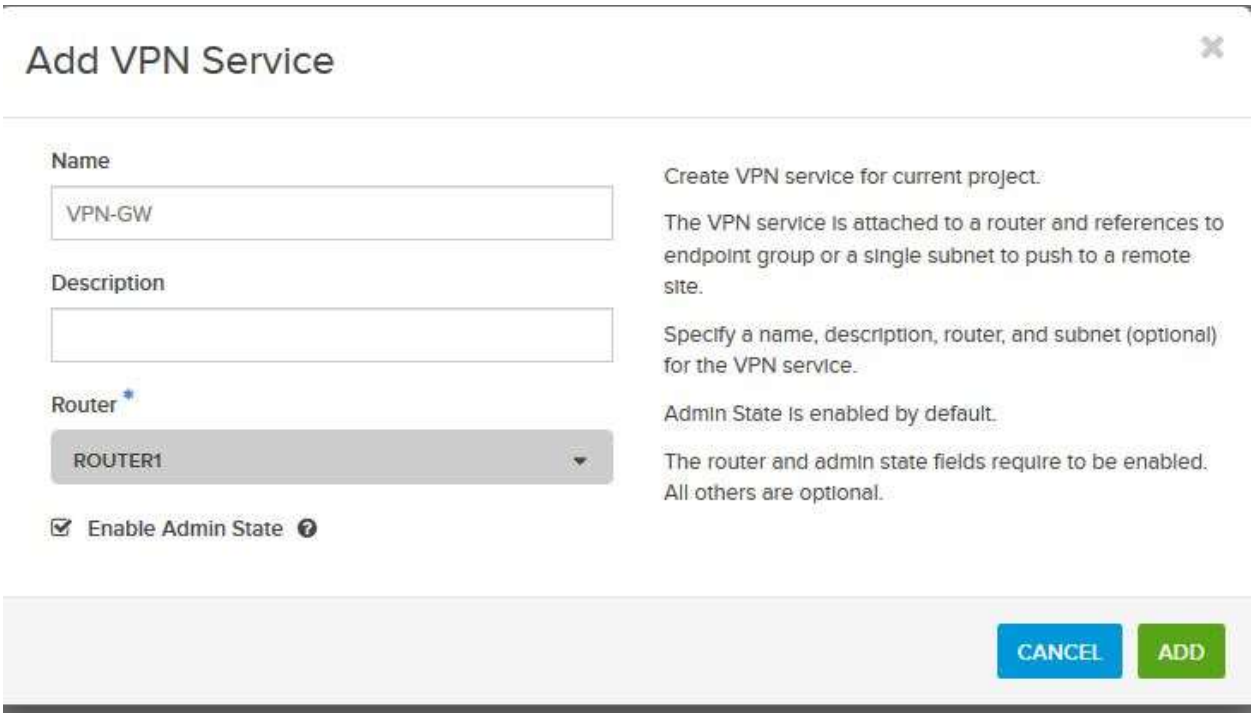
Valitse Ipsec Policies -välilehti ja lisää uusi Ipsec Policy: **+ ADD IPSEC POLICY**

Lisää Ipsec Policyyn kuvaava nimi ja lisää halutut parametrit salaukseen alasvetovalikoista sekä hyväksy policy **ADD** -painikkeella.



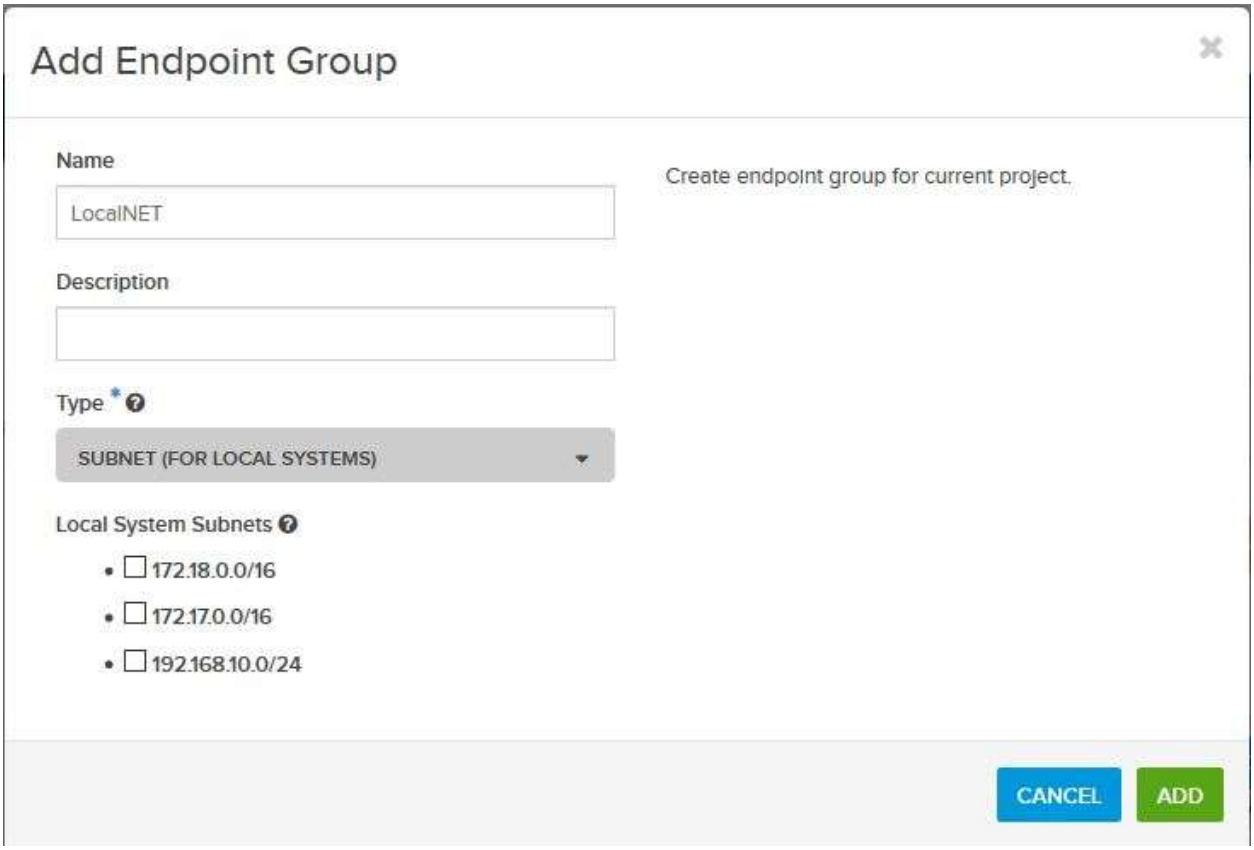
Valitse VPN Services välilehti ja Lisää uusi VPN Service: **+ ADD VPN SERVICE**

Anna VPN Servicelle kuvaava nimi ja valitse mitä reititintä Service käyttää (Reititin tulee olla luotu ennestään) Tämä VPN Servicen osoite on samalla VPN-tunnelissa oleva GW:n osoite ulospäin.

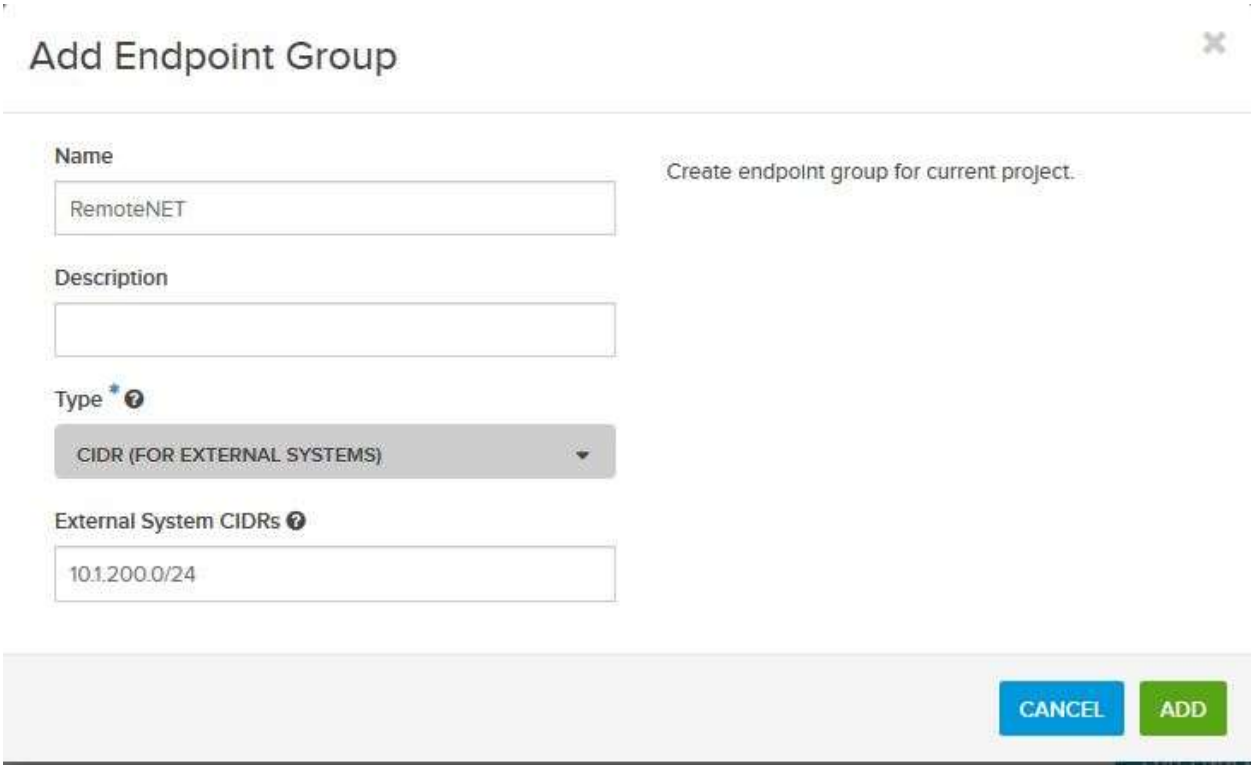


Valitse Endpoint Groups -välilehti ja lisää uusi Endpoint Group: **+ ADD ENDPOINT GROUP**

Luo INCloud9 ympäristössä olevasta subnetistä Endpoint Group. Nimeä haluamallasi nimellä ja valitse tyypiksi: SUBNET (FOR LOCAL SYSTEM) sekä valitse haluttu verkko.



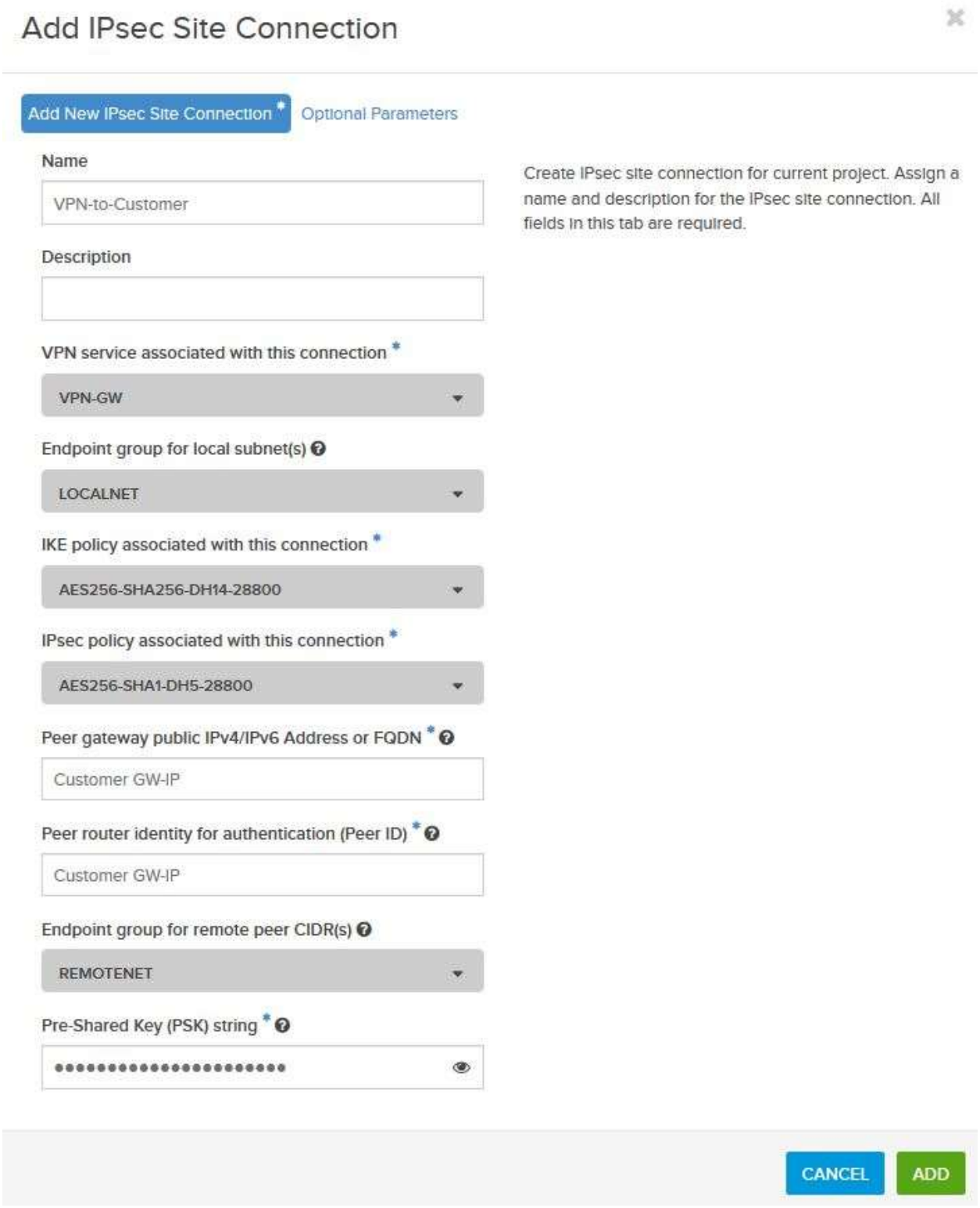
Luo Remote-puolen ympäristössä olevasta subnetistä Endpoint Group. Nimeä haluamallasi nimellä ja valitse tyypiksi: CIDR (FOR EXTERNAL SYSTEM) sekä kirjoita verkko-alue.



Valitse IPsec Site Connection välilehti, jossa yhdistetään kaikki edellä tehty VPN-tunneliksi. Lisää uusi Ipsec Site Connection: **+ ADD IPSEC SITE CONNECTION.**

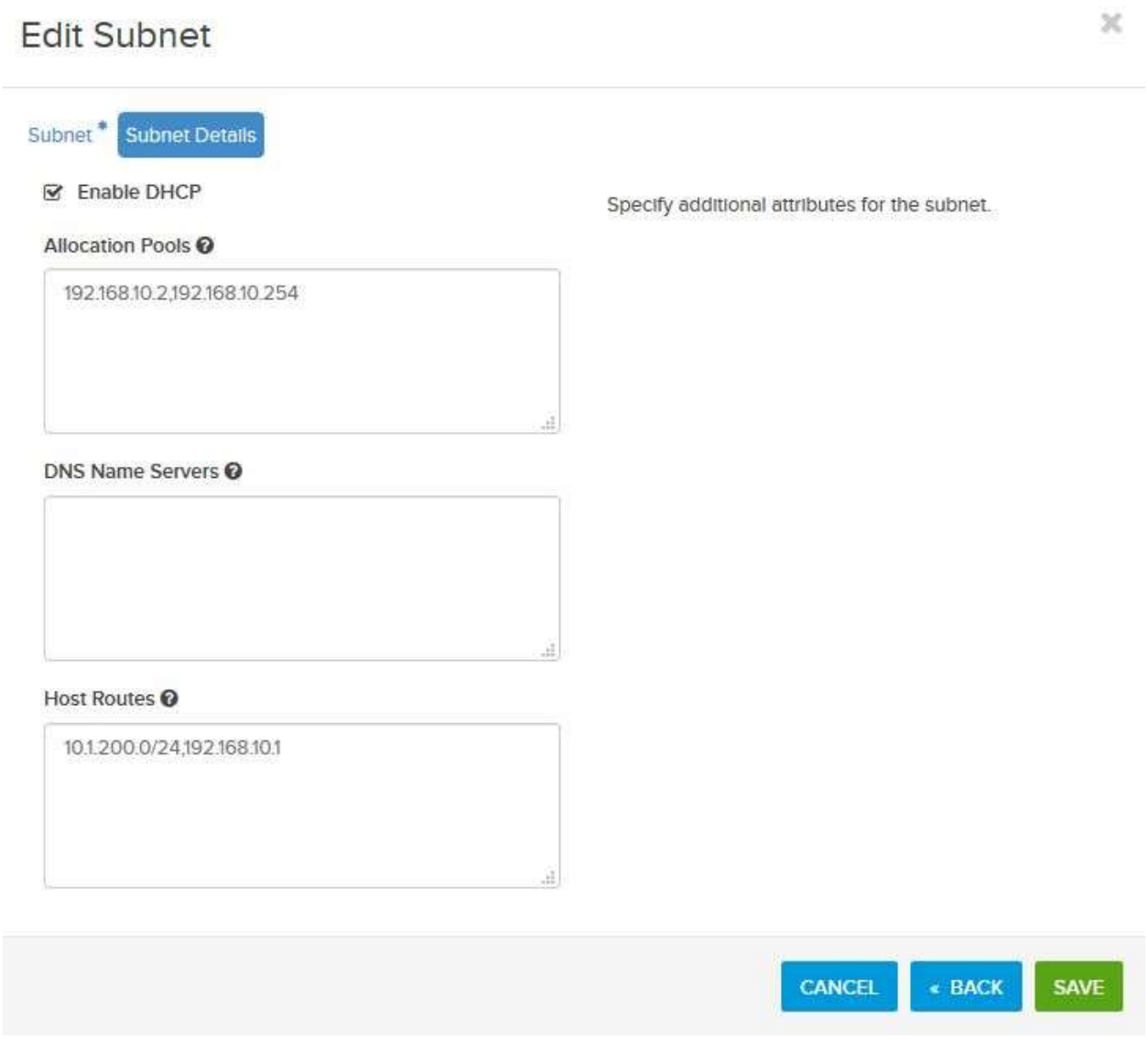
Nimeä Tunneli kuvaavalla nimellä ja valitse alasvetovalikoista aiemmin tehdyt asetukset.

Lisää kohde palomuurin osoite Peer Gateway -kohtaan. Hyväksy muutokset **ADD**-painikkeella.



Lopuksi verkkojen välille täytyy tehdä reitityssääntö, ja sen saa tehtyä Networks -> Valitaan ”LocalNET”-> Subnets -> Edit Subnet-> Subnet Detail ja lisätään Host Routes -kohtaan reitityssääntö.

RemoteSubnet, GW



Tämän jälkeen INcloud 9 -ympäristössä on kaikki tarpeellinen asetettu ja voi ruveta tekemään toiseen päähän tunnelia vastaavilla parametreillä. Alla komennot Juniperille.

JUNIPER SRX

set security ike proposal AES256-SHA256-DH14-28800SEC authentication-method pre-shared-keys
set security ike proposal AES256-SHA256-DH14-28800SEC dh-group group14
set security ike proposal AES256-SHA256-DH14-28800SEC authentication-algorithm sha-256
set security ike proposal AES256-SHA256-DH14-28800SEC encryption-algorithm aes-256-cbc
set security ike proposal AES256-SHA256-DH14-28800SEC lifetime-seconds 28800
set security ipsec proposal AES256-SHA256-128-ESP-3600sec protocol esp
set security ipsec proposal AES256-SHA256-128-ESP-3600sec authentication-algorithm hmac-sha-256-128
set security ipsec proposal AES256-SHA256-128-ESP-3600sec encryption-algorithm aes-256-cbc
set security ipsec proposal AES256-SHA256-128-ESP-3600sec lifetime-seconds 3600

```
set security ike policy TO-CLOUD9_VPN mode main
set security ike policy TO-CLOUD9_VPN proposals AES256-SHA256-DH14-28800SEC
set security ike policy TO-CLOUD9_VPN pre-shared-key ascii-text "PSK"
set security ike gateway TO-CLOUD9_VPN ike-policy TO-CLOUD9_VPN
set security ike gateway TO-CLOUD9_VPN address 1.2.3.4
set security ike gateway TO-CLOUD9_VPN no-nat-traversal
set security ike gateway TO-CLOUD9_VPN local-identity inet 4.3.2.1
set security ike gateway TO-CLOUD9_VPN remote-identity inet 1.2.3.4
set security ike gateway TO-CLOUD9_VPN external-interface ge-0/0/0.0
set security ike gateway TO-CLOUD9_VPN version v1-only
set security ipsec policy TO-CLOUD9_VPN perfect-forward-secrecy keys group14
set security ipsec policy TO-CLOUD9_VPN proposals AES256-SHA256-128-ESP-3600sec
set security ipsec vpn TO-CLOUD9_VPN bind-interface st0.X
set security ipsec vpn TO-CLOUD9_VPN ike gateway TO-CLOUD9_VPN
set security ipsec vpn TO-CLOUD9_VPN ike idle-time 60
set security ipsec vpn TO-CLOUD9_VPN ike no-anti-replay
set security ipsec vpn TO-CLOUD9_VPN ike ipsec-policy TO-CLOUD9_VPN
set security ipsec vpn TO-CLOUD9_VPN ike install-interval 1
set security ipsec vpn TO-CLOUD9_VPN traffic-selector "name" local-ip 10.1.200.0/24
set security ipsec vpn TO-CLOUD9_VPN traffic-selector "name" remote-ip 192.168.10.0/24
set security ipsec vpn TO-CLOUD9_VPN establish-tunnels immediately
```

Alaotsikko: INCLOUD: NELB-KUORMANTASAUS

Nebula Elastic LoadBalancerin eli NELB:in voi ottaa käyttöön Cloud9:n hallinnasta tai vaihtoehtoisesti käyttäen NELB:in hallintaan tarkoitettu API-rajapintaa.

Cloud9 projekteilla on oletuksena rajattu 5 kpl NELB-kuormantasaajia ja 50 kpl SSL-sertifikaattiketjuja. Rajojen nostoa voi tarvittaessa pyytää asiakaspalvelumme kautta.

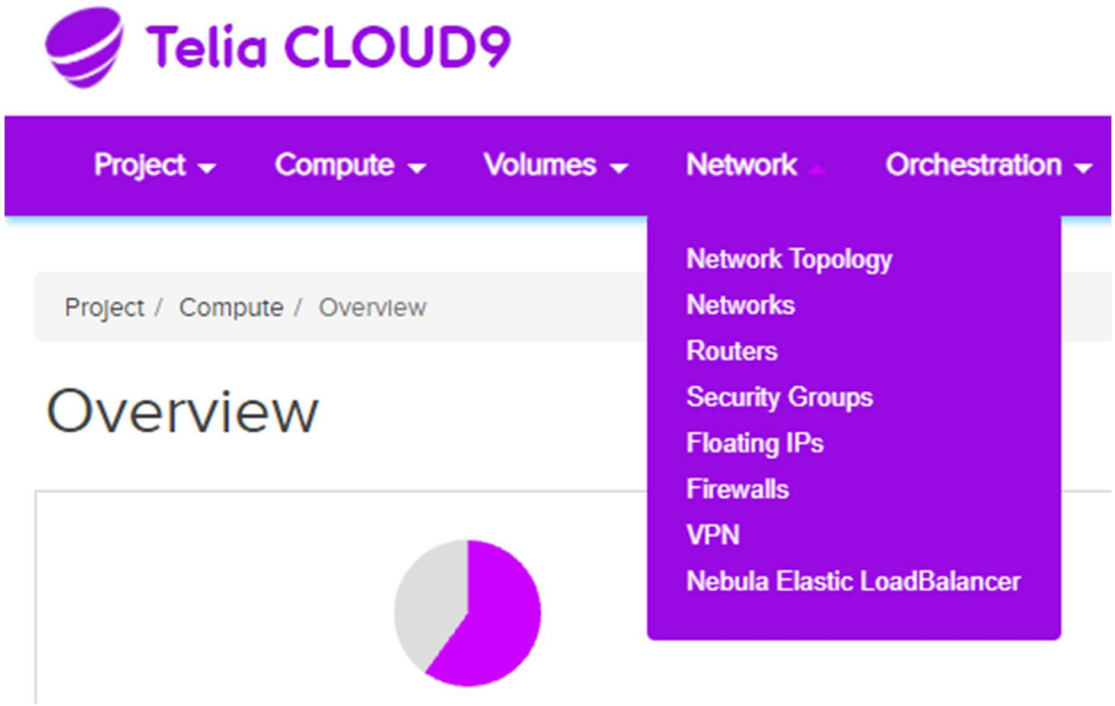
NELB API on Swagger 2.0 yhteensopiva rajapinta, jonka spesifikaatio löytyy osoitteesta: https://nelb.fi-1.nebulacloud.fi/v1/swagger.yml
Autentikoinnissa käytetään samaa OpenStack Keystone Tokenia (OS_TOKEN), kuin OpenStackClient-komentorivityökalujen kanssa autentikoituessa.

YLEISET TERMIT SELITETTYNÄ

Termi	**Selitys**
NELB	Nebula Elastic LoadBalancer -kuormantasauspalvelu
Member	Kuormantasattava palvelin. Näitä on yleensä monta esim. WWW-palvelimen muodossa, joiden ku

Termi	Selitys
Listener	Kuormantasaajan kuuntelema portti, josta liikenne ohjataan Memberille.
Admin State	Kuormantasaajan eli NELB:in “virtakatkaisin”. **HUOM!** Tämä ei vaikuta laskutukseen.
Default Policy	NELB Listenereiden oletusasetukset.
Default Certificates	NELB Listenereiden oletussertifikaatit.
Listener Policy	Yksittäisen Listenerin erilliset asetukset, jotka yliajavat oletusasetukset.
Listener Certificates	Yksittäisen Listenerin erilliset sertifikaatit, jotka yliajavat oletussertifikaatit.
Member Weight	Yksittäisen Memberin painoarvo 0-256 välillä. 0 = Member on pois käytöstä.

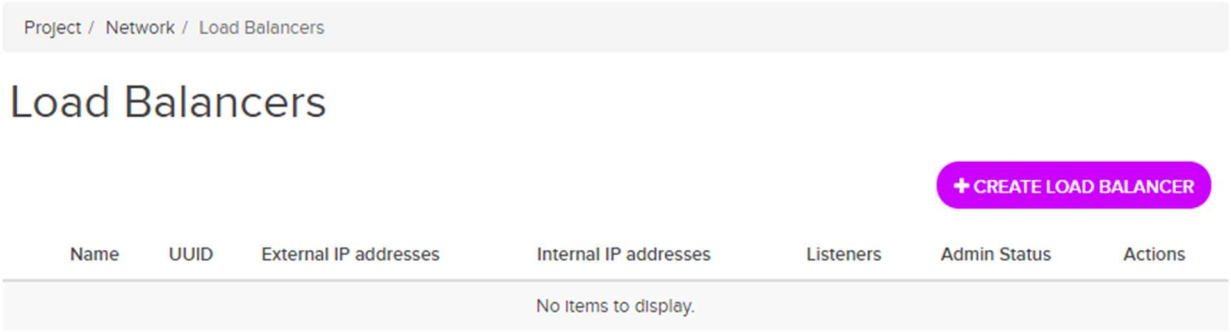
NELB-KUORMANTASAUS **(NETWORK -> NEBULA ELASTIC LOADBALANCER)**



Uuden NELB:in voi luoda klikkaamalla ”**Create Load Balancer**” ja nimen määrityksen jälkeen ”**Save changes**”, jonka jälkeen NELB provisioituu projektille ja käynnistää automaattisen On-Demand laskutuksen.

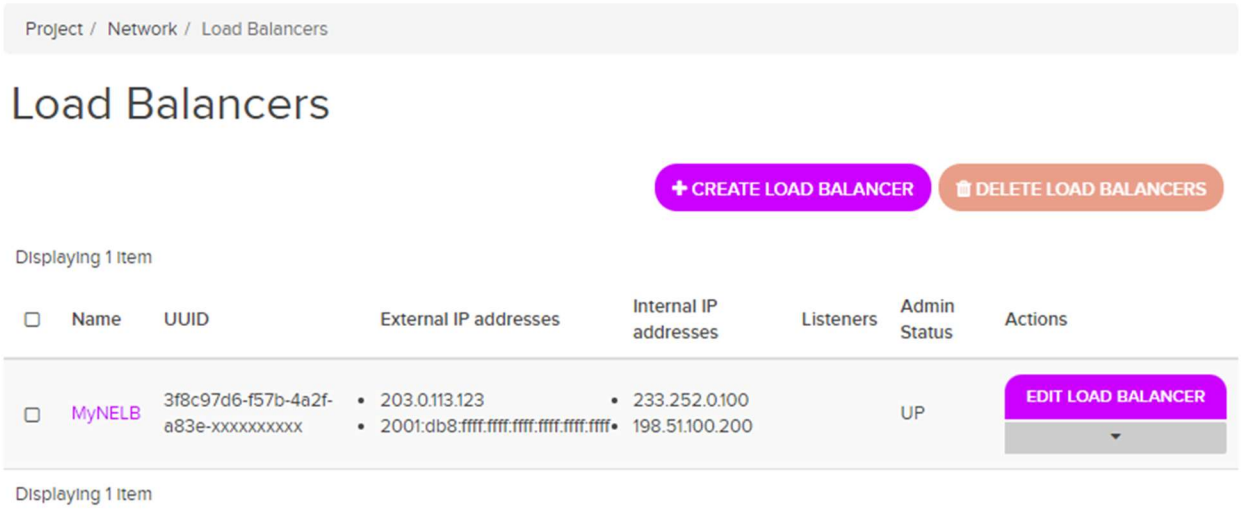
Provisionnissa projektille varataan kahdennettu NELB-instanssi, joka sisältää yhden julkisen IPv4-osoitteen, yhden julkisen IPv6-osoitteen ja kaksi sisäistä IPv4-osoitetta, joista liikenne saapuu kohdepalvelimelle.

Sisäiset IP-osoitteet on sallittava instanssien palomuuriasetuksista (mm. Security Groupilla ja ohjelmistopalomuurista), jotta NELB voi liikennöidä **Memberien** kanssa.



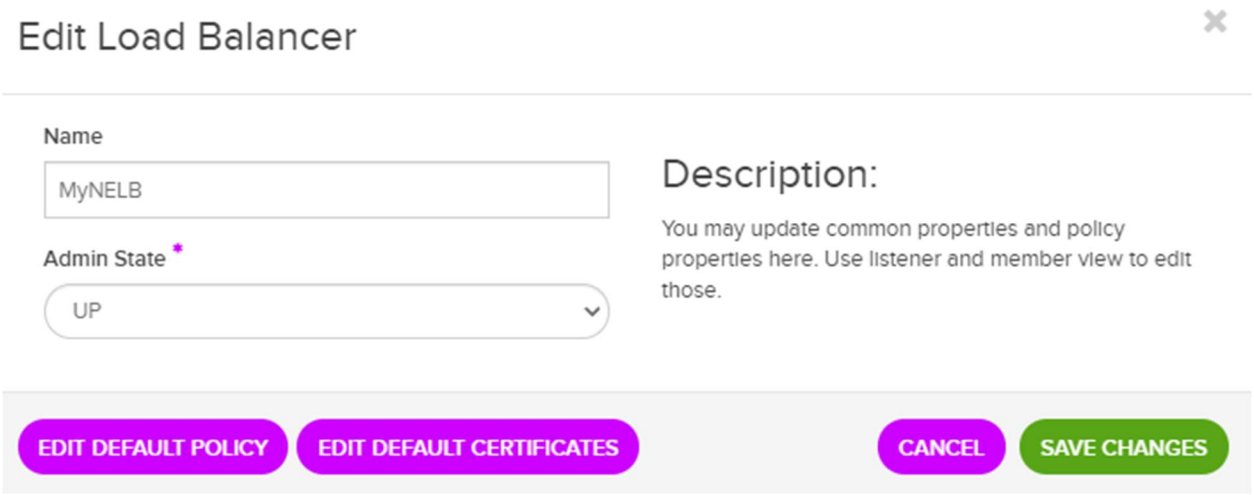
NELB:in provisioiduttua se ilmestyy alla näkyvään listaan, josta sen asetuksia pääsee muokkaamaan joko klikkaamalla ”**Edit load balancer**” ja klikkaamalla sen nimestä **Listener** ja **Member**-määrityksiä varten.

Tässä esimerkissä NELB:in julkinen IPv4-osoite on 203.0.113.123, jonka voi määrittää esimerkiksi verkkotunnuksen DNS-tietueeseen.
Sisäiset IPv4-osoitteet ovat 233.252.0.100 ja 198.51.100.200, jotka on sallittava kohdepalvelimien päästä. NELB:in julkiseen IP-osoitteeseen kohdistuva liikenne näkyy kuormantasatuille palvelimille näistä sisäisistä IPv4-osoitteista (yhteyden todellinen IP-osoite on mahdollista saada, ohjeessa alempana lisää asiasta).



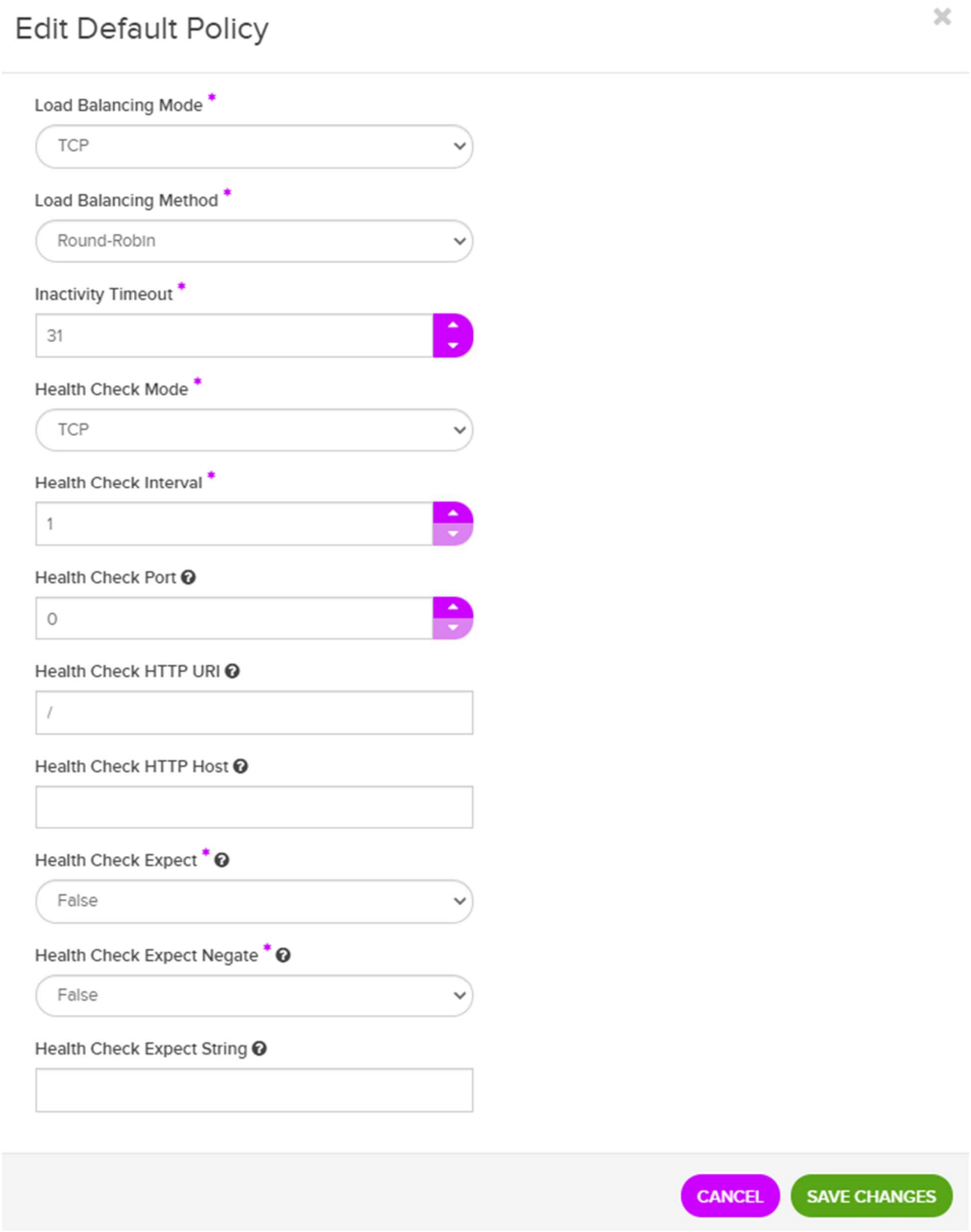
NELB:in asetuksien kautta pystyy muun muassa asettamaan NELB:in inaktiiviseksi (**Admin State**), määrittämään kuormantasauksen tyypin ja tilan (**Edit Default Policy**) sekä liittämään MyNebulan kautta lisättyjä SSL-sertifikaatteja NELB:in SSL-purkua varten (**Edit Default/Listener Certificates**).

HUOM! NELB:in laskutus ei pysähdy vaikka sen asettaisi inaktiiviseksi. On-Demand laskutus perustuu projektille varattuihin resursseihin ja kapasiteettiin.



NELB:IN OLETUSKONFIGURAATIO **(EDIT DEFAULT POLICY)**

Asetukset ja vaihtoehdot on selitetty tarkemmin kuvan alapuolella.



Default Policyn asetukset ja vaihtoehdot selitettynä:

- **Load Balancing Mode**

- **TCP:** Layer 4 kuormantasaus, jossa TCP-paketit ohjataan suoraan Memberille.
- **HTTP:** Layer 7 kuormantasaus, jossa yhteys ohjataan Memberille samalla HTTP Headerit säilyttäen.
- **TCP-Proxy:** Layer 7 yhteensopiva kuormantasaus, jolla on mahdollista kuljettaa mm. HTTP Headerit, myös salattuna.

  Tällä pystyy toteuttemaan mm. SSL-purun Memberillä NELB:in sijaan, mutta Memberin ohjelmiston on tuettava **HAProxy Proxy Protocol** -kommunikaatiota.

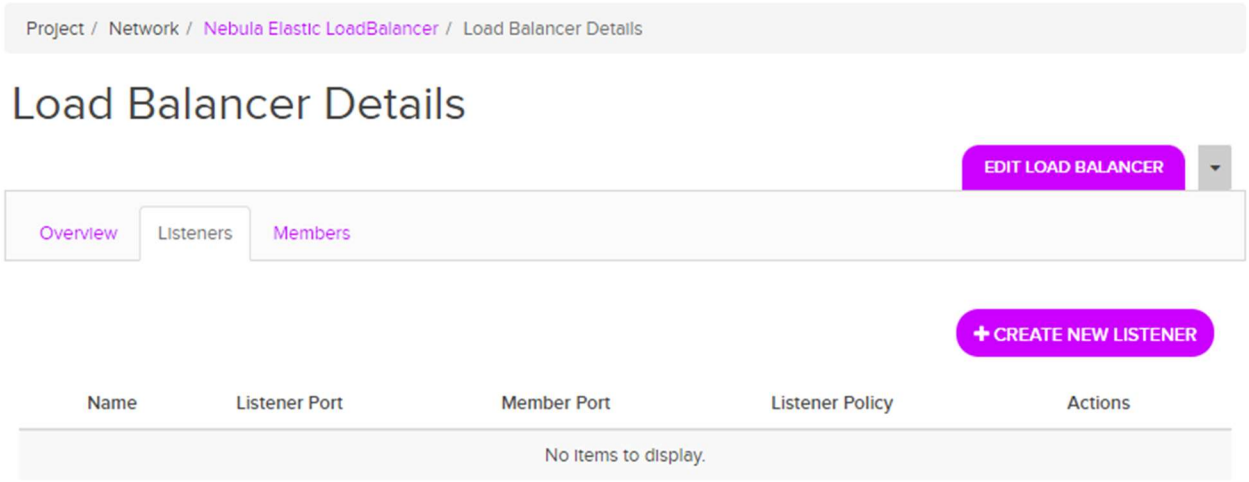
  - **Lisätietoja:** https://www.haproxy.com/blog/haproxy/proxy-protocol/
  - **Dokumentaatio:** https://www.haproxy.org/download/1.8/doc/proxy-protocol.txt
  - **Proxy Protocol Apache 2.4.31+:** https://httpd.apache.org/docs/2.4/mod/mod_remoteip.html#remoteipproxyprotocol
  - **Proxy Protocol Nginx 1.13.11+:** https://docs.nginx.com/nginx/admin-guide/load-balancer/using-proxy-protocol/
  - **Apache TomCat:** Ei tuettu – https://bz.apache.org/bugzilla/show_bug.cgi?id=57830
  - **Microsoft IIS:** Ei tuettu
- **Load Balancing Method**
  - **Round-Robin**: Tasaa yhteyksiä Memberin kuormituksen ja Weight-arvon perusteella.
  - **Least Connections**: Ohjaa yhteyden pienimällä kuormituksella olevalle Memberille.
  - **Source IP Address**: Ohjaa yhteyden samalle Memberille yhteyden avaajan IP-osoitteen perusteella.
    HUOM! Tämä ei ole sama asia, kuin ”Sticky session”. Tämä logiikka on toteutettava NELB:in ulkopuolella.
- **Inactivity Timeout**
  - Aikakatkaisun pituus sekunneissa, kunnes avoin liikennöimätön yhteys katkaistaan.
- **Health Check Mode**
  - **TCP:** Tarkistuksessa tarkistetaan Memberin portin vastaaminen.
  - **HTTP:** Tarkistuksessa tarkistetaan Memberin palauttama HTTP status code.

        - **Health Checks Disabled:** Kaikki Memberit ovat aina käytössä toimivuudesta riippumatta.
    - **Health Check Interval**
        - Tarkastuksien välinen viive sekunneissa.
    - **Health Check Port**
        - Tarkastukseen käytettävän TCP-portin numero. Mikäli tyhjä tai ”0”, tarkastuksessa käytetään Memberin porttia/portteja.
    - **Health Check HTTP URI**
        - HTTP GET pyynnöllä tehtävän tarkistuksen URI-osoite, jonka on vastattava HTTP 2XX/3XX normaalissa tilanteessa.
        - **HUOM!** Tämän arvon on oltava vähintään “/” vaikka Health Check ei olisi käytössä. Tyhjästä tai väärästä arvosta aiheutuu virhe asetuksia tallentaessa.
    - **Health Check HTTP Host**
        - HTTP GET pyynnössä käytettävä ”Host” header. Tämä voi olla hyödyllinen, mikäli tarkistus halutaan esimerkiksi ajaa tiettyyn sivustoon verkkotunnuksen/hostnamen perusteella.
    - **Health Check Expect**
        - HTTP GET pyynnön vastaanotetun datan (body) tarkistus, jossa kuormantasattu palvelin vastaa tietyn tekstin (string) tarkistuksen yhteydessä.
        - Mikäli tämä ei ole käytössä, Membereistä tarkistetaan vain HTTP 2XX/3XX vastausta eikä vastaanotetun datan sisältöä.
    - **Health Check Expect Negate**
        - Alemman määrityksen negaatio eli Memberille ei ohjata yhteyksiä, mikäli Memberin palauttama data (body) täsmää.
    - **Health Check Expect String**
        - Memberin HTTP GET pyynnön vastaanotettavan datan (body) täsmällinen arvo. Isot ja pienet kirjaimet on myös täsmättävä eli tarkistus on ns. Case-Sensitive. **HUOM!** Älä määritä tähän HTTP Headereita vastaanotettavan datan (body) lisäksi.

CREATE NEW LISTENER

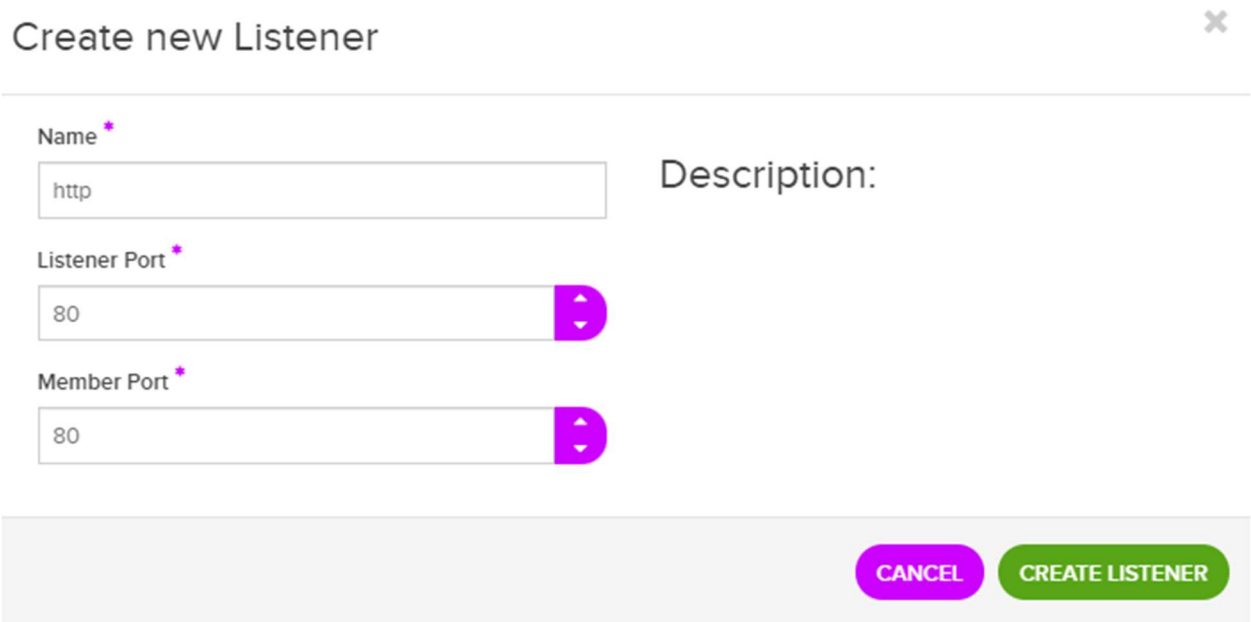
Listeners-välilehdeltä voi määrittää Listenereitä eli ulospäin näkyviä portteja, joista yhteydet ohjataan Membereille.
Yksittäiselle **Listenerille** voi määrittää myös erillisen **Listener Policyn**, joka yliajaa **Default Policyn** määritykset.

Listener Policyä voi muokata sen jälkeen, kuten Listener on luotu (**Edit Listener**).
Listener Policyn voi poistaa valinnasta "**Revert to Default Policy**".



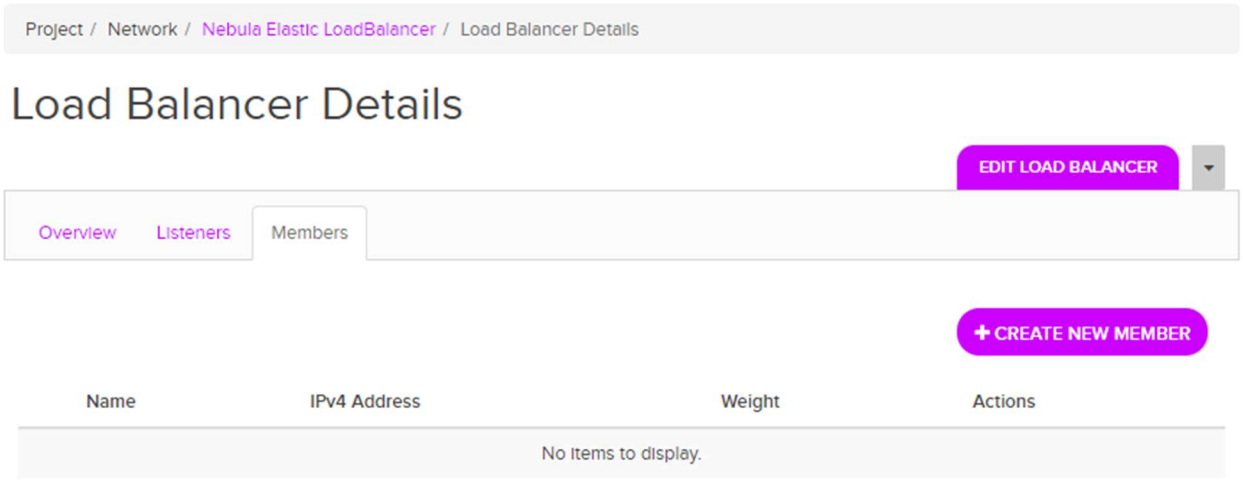
Tässä esimerkiksi HTTP-yhteyksien ohjaamiseen tarkoitettu **Listener**, jolla NELB:in Julkinen IP-osoite vastaa portilla 80 (HTTP) ja ohjaa liikenteen **Memberin** porttiin 80 (HTTP). Porttien ei tarvitse olla samat Listenerin ja Memberin kesken.

Standardiporttien numerot löytyvät mm. täältä (https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)



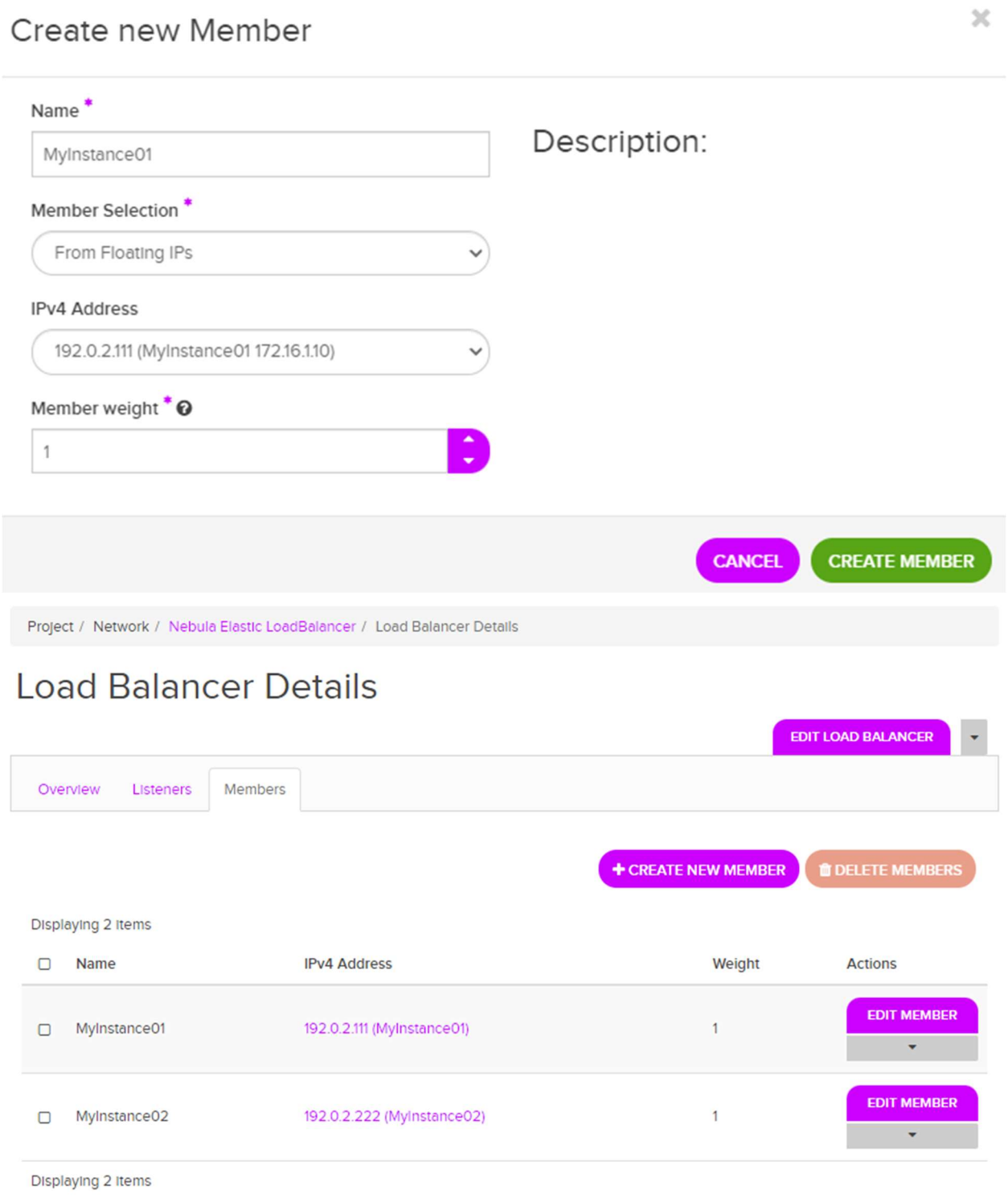
CREATE NEW MEMBER

Listenereitä varten tarvitaan myös **Membereitä** eli osoitteita, joihin NELB ohjaa liikenteen mikäli esim. **Default Policyn** tai **Listener Policyn** ehdot (Health Check) täyttyvät.



Memberiksi voi määrittää esimerkiksi suoraan instanssin sen Floating IP:n perusteella.
Member weight arvolla voi määrittää Memberin painoarvon suhteessa muihin Membereihin. Mikäli arvo on sama kaikilla Membereillä, yhteydet ohjataan tasa-arvoisesti kaikkien Membereiden välillä.

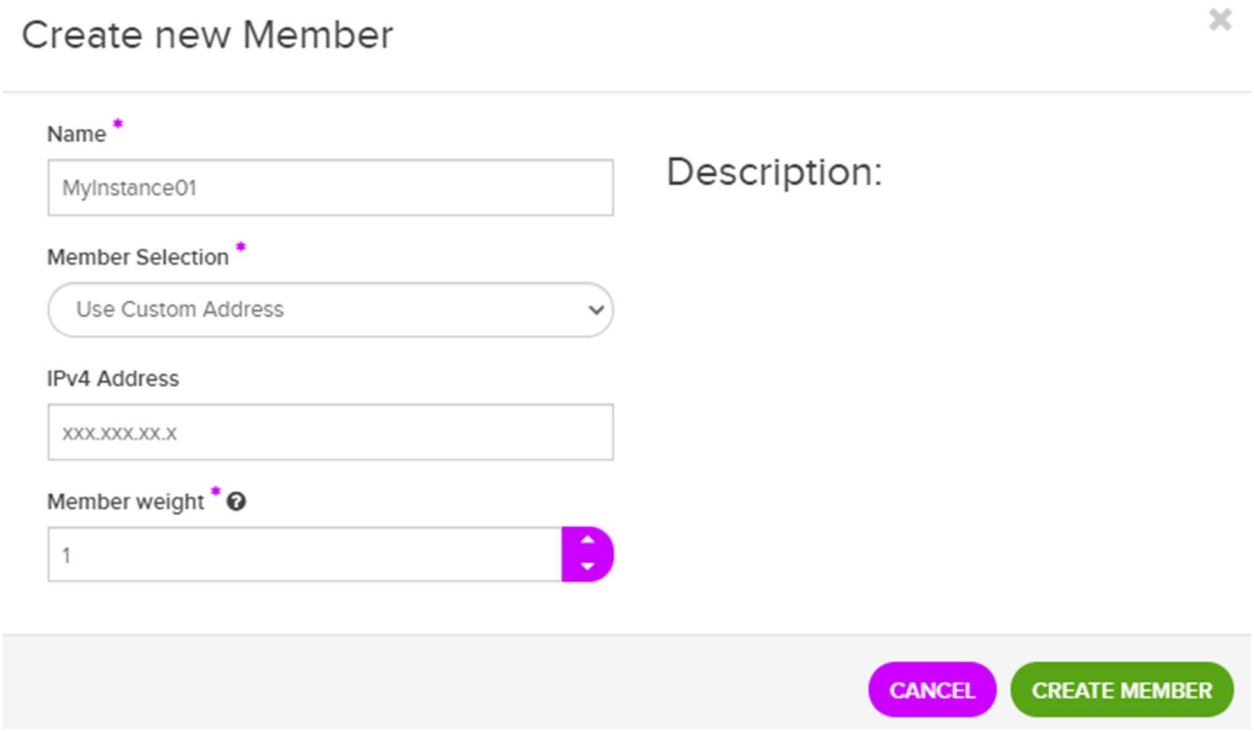
HUOM! Varmista, että NELB:in Internal IP-osoitteet on sallittu kohteen päässä.



Voit myös vaihtoehtoisesti valita kohteeksi IP-osoitteen, johon yhteydet ohjataan. IP-osoitteeksi kelpaa myös muissa alustoissa ja palveluntarjoajilla sijaitsevat palvelimet.

Tämä määritys voi olla hyödyllinen silloin, kun IP-osoite siirtyy usein toiselle instanssille tai jos ympäristö halutaan toteuttaa automaattisesti skaalautuvaksi NELB:in kanssa.

HUOM! Varmista, että NELB:in Internal IP-osoitteet on sallittu kohteen päässä.

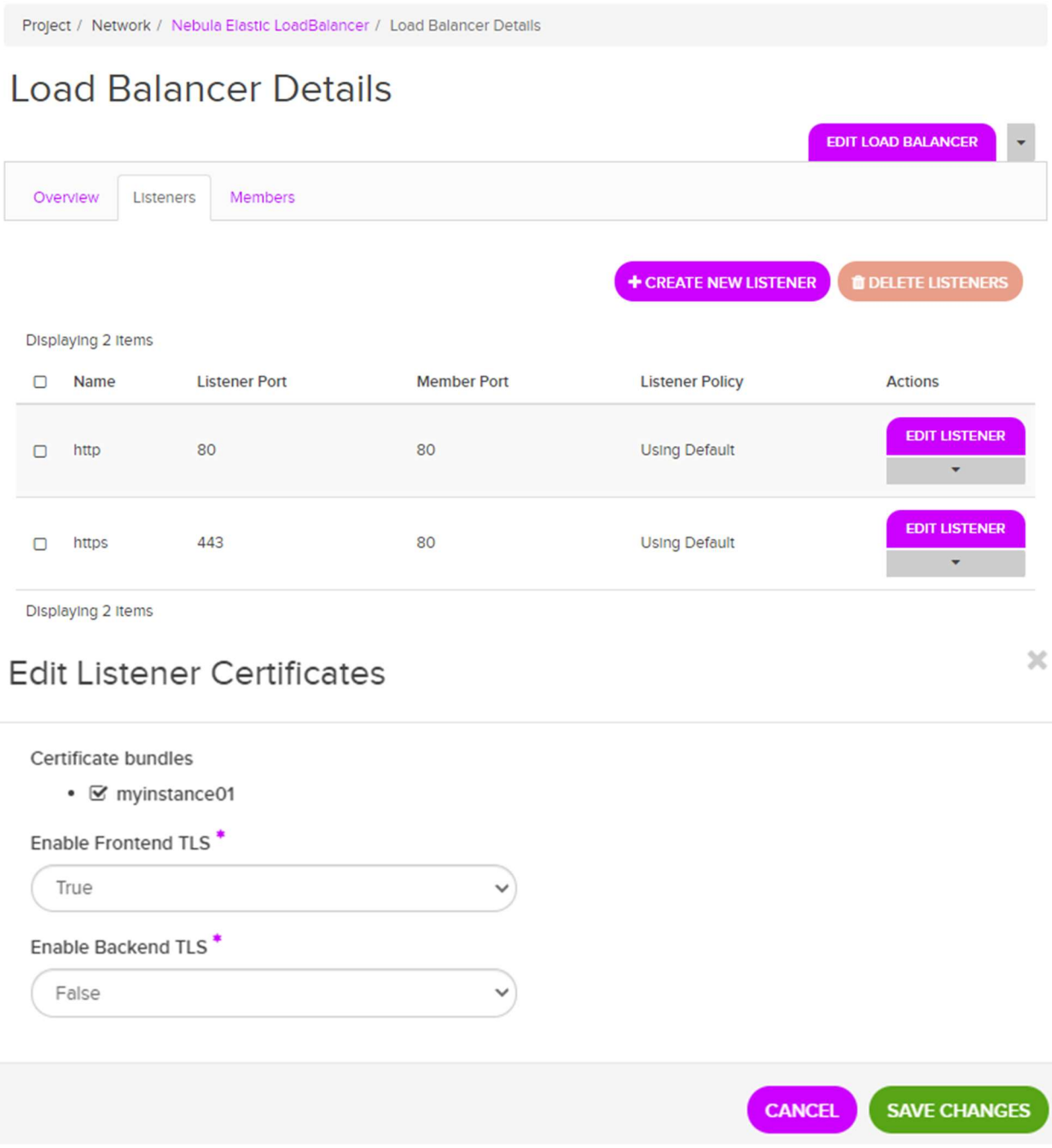


NELB-KUORMANTASAUS SSL-SUOJAUKSELLA (HTTPS)

Vaihtoehto 1

- Lisää SSL-sertifikaatti sopimuksellesi MyNebulasta käsin ja linkitä SSL-sertifikaatti tarvitsemaasi Cloud9 projektiin.
  Ohjeet tähän löytyvät tukikeskuksen sivulta MyNebula: SSL-sertifikaatit.
- Varmista, että NELB:istä löytyy Listener, joka ohjaa Listener portin 443 liikenteen Memberin porttiin 80 (alempana esimerkki).
- **HUOM!** Mikäli haluat HTTPS-yhteyden todellisen IP-osoitteen (“X-Forwarded-For” headerin), niin määritä Listener portti 443 Listener Policy erikseen Load Balacing Mode = HTTP -tilaan.
  Listener policy menee automaattisesti TCP-tilaan, kun Listenerille määrittää erikseen sertifikaatin.
- Liitä projektille linkitetty SSL-sertifikaatti NELB:iin ja ota TLS/SSL käyttöön seuraavasti:

1. **Edit Load Balancer** -> **Listeners** -> [Itse luomasi HTTPS listener] -> **Edit Listener** -> **Edit Listener Certificates**



2. Valitse “**Certificate Bundles**” otsikon alta käyttöön otettavat sertifikaatit. Tässä esimerkissä “myinstance01” on sertifikaatin Common Name (CN).

3. Määritä ”**Enable Frontend TLS**” tilaan ”**True**”

4. Määritä “**Enable Backend TLS**” tilaan “**False**”

5. Tallenna asetukset “**Save changes**” painikkeesta ja testaa suojattua yhteyttä NELB:in julkisen IP-osoitteen kautta.

Vaihtoehto 2

- Asenna SSL-sertifikaatti (esim. Let’s Encrypt) kohdepalvelimiin (esim. Apache2 tai Nginx).
- Konfiguroi kohdepalvelimet käsittelemään HAProxy Proxy Protocol -yhteyksiä.

Esimerkki Apache versiossa 2.4.31 ja uudemmissa (dokumentaatio)

RemoteIPProxyProtocol On

RemoteIPTrustedProxy 233.252.0.100 -> NELB:in sisäinen IPv4-osoite.

RemoteIPTrustedProxy 198.51.100.200 -> NELB:in toinen sisäinen IPv4-osoite.

RemoteIPProxyProtocolExceptions 127.0.0.1 ::1 -> Tähän listaan voi määrittää poikkeuksia, jolloin Proxy Protocol ei ole käytössä, niin yksittäisen instanssin sivuston toimivuuden voi testata suoraan instanssin IP-osoitteella.

Esimerkki Nginx versiossa 1.13.11 ja uudemmissa (dokumentaatio)

listen 443 ssl http2 proxy_protocol;

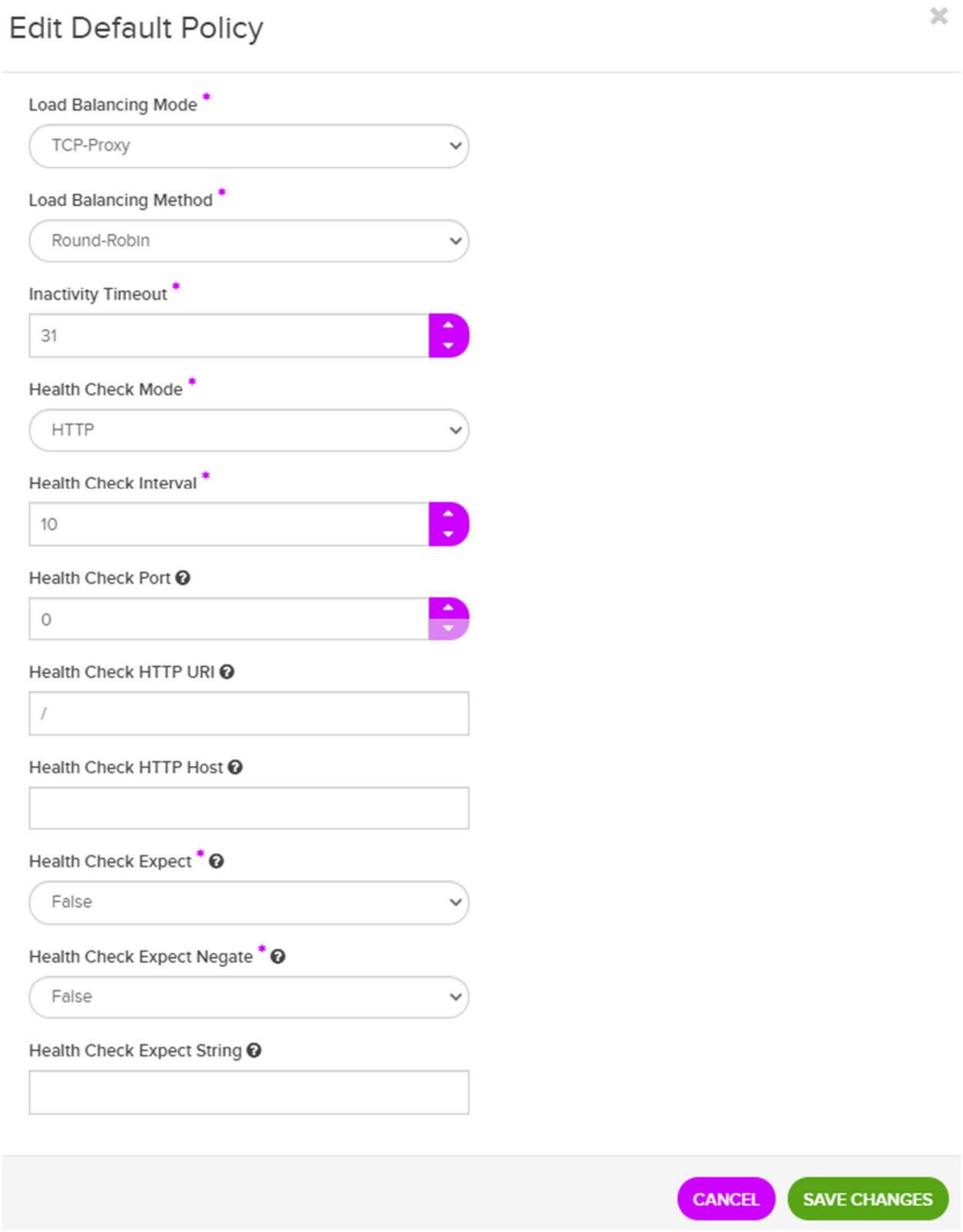
set_real_ip_from 233.252.0.100; -> NELB:in sisäinen IPv4-osoite.

set_real_ip_from 198.51.100.200; -> NELB:in toinen sisäinen IPv4-osoite.

real_ip_header proxy_protocol; -> HTTP Headerin NELB:in sisäinen IP-osoite korvataan todellisella IP-osoitteella.

- Määritä NELB:in ”**Load Balancing Mode**” tilaan ”**TLS-Proxy**” ja määritä tarvittaessa esim. HTTP Health Check.

  Esimerkki NELB Default Policy HTTP ja HTTPS-yhteyksiä varten HTTP Health Checkin kanssa



Testaa yhteyksiä NELB:in julkisen IP-osoitteen (esimerkissä 203.0.113.123) kautta kohdepalvelimille (esimerkissä MyInstance01 [192.0.2.111] ja MyInstance02 [192.0.2.222]).

Kaikkien Membereiden toimivuutta voi testata esimerkiksi nostamalla yhden Memberin painoarvoa (**Member weight**) väliaikaisesti korkeammaksi.

Health Checkin toimivuus on myös hyvä testata esim. sammuttamalla Memberiltä kuormantasattu sovellus tai muuttamalla mahdollisen HTTP Health Checkin palauttamaa arvoa väliaikaisesti, mikäli “Except String” on käytössä.

Alaotsikko: INCLOUD: LEVYTILAN KÄYTTÖ

Volumet ovat vikasietoisilla levyjärjestelmillä sijaitsevaa massamuistia jotka voidaan liittää yhteen palvelimeen kerrallaan. Volume näkyy kovalevynä palvelimelle, ja sitä voi vapaasti käsitellä haluamallaan tavalla (partitiointi, tiedostojärjestelmät, LVM jne). Volumeja voi myös kasvattaa. Useasta volumesta voi käyttöjärjestelmässä tehdä Stripe-menetelmällä yhden isomman loogisen levyjaon, ja volumen voi sen omistavasta palvelimesta jakaa eteenpäin muille palvelimille käyttöjärjestelmästä (NFS/CIFS/iSCSI ym).

Levytilan luomiseen tarvitaan kolme tietoa:

- Käytettävä saatavuusalue
- Volumen koko
- Volumen nopeusluokka

Luomisen jälkeen volumen voi liittää yhteen palvelimeen kerrallaan.

Volumen voi irrottaa kyseisestä palvelimesta ja sen jälkeen liittää toiseen palvelimeen. Tämä on hyödyllistä esimerkiksi tilanteissa, missä käyttöjärjestelmän vaihdossa tai päivityksessä tehdään rinnalle korvaava instanssi, yliheitossa vanha instanssi sammutetaan ja siihen kiinnitetty volume kiinnitetään uuteen instanssiin. Näin sama data on heti uudella palvelimella käytettävissä.

Käyttötarpeesta riippuen volumen ominaisuuksiin kannattaa kiinnittää huomiota. Esim halvin ja hitain arkistointipinta ei ole paras mahdollinen valinta esimerkiksi tietokantakäyttöön, ja vaihtoehtoisesti kallista SSD-pintaa on turhaa varata varmuuskopioiden säilömiseen.

Palveluita suunnitellessa kannattaa kiinnittää alusta asti huomiota tilantarpeeseen ja datan sijoitteluun. Jälkikäteen tietyn sovelluksen siirtäminen volumelle tai eri hakemistoon palvelimella tarkoittaa pahimmillaan huoltokatkoa tai muutoksia sovelluksen koodiin.

Volumeista voi ottaa snapshoteja ja uusia volumeja voi luoda käyttäen lähteenä volume-snapshotia. Näin saman datan voi kopioida useaan volumeen tai snapshotin kopioimalla jopa nopeusluokasta toiseen.

Volumet toimivat vain omalla saatavuusalueellaan, et voi kiinnittää Helsinki-1 -zonella asuvaa volumea Helsinki-2 –zonella sijaitsevaan palvelimeen.

SUORITUSKYKYRAJAT

Palvelimille on määritelyt IO-rajat. Rajojen tarkoitus on varmistaa että kaikki asiakkaat saavat tehoja saman verran, eikä ikävää “noisy neighbour” efektiä ilmene. Näin asiakkaat voivat olla luottavaisia että suorituskyky on hyvin samanlainen jos käytössä on useita samanalaisia palvelimia. Rajojen määrittelyssä on huomioitu, että yleensä järeämpi palvelin tarvitsee myös enemmän levy IO:ta.

ResurssitKOKOONPANO

IOPS (R)IOPS (W)IO MB/sCPU painoNimi

40030050512nbl-f1-micro1 CPU, 1Gt, 32 järjestelmälevyä

40030050512nbl-n1-tiny1 CPU, 1Gt, 8Gt järjestelmälevyä

800500801024nbl-n1-small1 CPU, 2Gt, 32Gt järjestelmälevyä

10006001001024nbl-m1-small1 CPU, 4Gt, 50Gt järjestelmälevyä

15006001001024nbl-n1-medium2 CPU, 4Gt, 50Gt järjestelmälevyä

30007001251536nbl-m1-medium2 CPU, 8Gt, 50Gt järjestelmälevyä

40007001501536nbl-n1-large4 CPU, 8Gt, 100Gt järjestelmälevyä

40007001501536nbl-m1-large4 CPU, 16Gt, 100Gt järjestelmälevyä

40007001501536nbl-n1-xlarge8 CPU, 16Gt, 100Gt järjestelmälevyä

40008001501536nbl-m1-xlarge8 CPU, 32Gt, 150Gt järjestelmälevyä

40008001502048nbl-n1-2xlarge16 CPU, 32Gt, 150Gt järjestelmälevyä

40008001502048nbl-m1-2xlarge16 CPU, 64Gt, 200Gt järjestelmälevyä

40008001501536nbl-hm1-large2 CPU, 16Gt, 100Gt järjestelmälevyä

40008001502048nbl-hm1-xlarge4 CPU, 32Gt, 150Gt järjestelmälevyä

40008001502048nbl-hm1-2xlarge8 CPU, 64Gt, 200Gt järjestelmälevyä

400010001502048nbl-hm1-4xlarge16 CPU, 128Gt, 300Gt järjestelmälevyä

ONGELMATILANTEITA

Esimerkkiongelma 1:

Sovelluspalvelimelle on luotu volume, nopeusluokka ARK (hitain) ja koko 500GB. Levyillä säilytetään dataa jota luetaan melko aktiivisesti. Levyn lukusuorituskyky ei ole riittävä sovelluksen tarpeisiin nähden, joka aiheuttaa ongelmia sovelluksessa. Lisäksi levytila alkaa olemaan vähissä.

Korjaus:

1. Tehdään uusi SAS-nopeusluokan volume, koko 800GB
2. Kiinnitetään SAS-volume palvelimeen

3. Pysäytetään sovellus hetkeksi levyä käyttävältä palvelimelta
4. Kopioidaan ARK-levyn sisältö SAS-levylle
5. Kun kopiointi valmis, pysäytetään / unmountataan / irroitetaan ARK-levy käyttöjärjestelmästä ja sen jälkeen hallintapaneelissa irroitetaan ARK-levy palvelimesta
6. Kiinnitetään käyttöjärjestelmässä SAS-levy sijaintiin missä ARK-levy oli
7. Käynnistetään sovellus
8. Jos kaikki toimii oikein, poistetaan ARK-volume.

Esimerkkiongelma 2:

Sovelluspalvelimella olevalta suurelta SAS-volumelta pitäisi saada kaikki tiedostot raportointipalvelimelle jatkokäsittelyä varten, mutta jatkuva kirjoitus estää kopioinnin, data muuttuu nopeammin kuin mitä kopiointiohjelma ehtii lukemaan ja kopio ei ole validi. Käsittely epäonnistuu.

Korjaus:

1. Otetaan levystä snapshot, nimetään se ”data-snap”
2. Luodaan uusi volume samalle LTK-levytasolle (LTK-SAS). Käytetään volumen lähteenä snapshotia ”data-snap”. Annetaan volumen nimeksi mielikuvituksellisesti ”data-volume”.
3. Kun uusi volume on valmistunut, poistetaan snapshot ”data-snap”.
4. Kiinnitetään tämä uusi volume raportointipalvelimeen ja käsitellään data.
5. Käsittelyn valmistuessa irroitetaan ja poistetaan data-volume.

Tämän esimerkin toimenpiteen voi myös skriptata ja ajastaa cinder-clientia käyttäen, näin raportointikäsittelyn voi automatisoida.

HUOM!

Emme suosittele irrottamaan volumea Pilven hallintapaneelissa mikäli se on edelleen palvelimen käyttöjärjestelmässä aktiivisena. Käyttöjärjestelmälle levyn irtoaminen on käytännössä sama kuin fyysinen kovalevy rikkoutuisi kesken luvun. Se saattaa aiheuttaa huomattavia ongelmia palvelimelle sekä kyseiselle volumelle.

KAPASITEETIN KÄYTTÖASTEEN / LEVYTYYPPIN TARKISTAMINEN

Parhaiten käytetyn levytilakapasiteetin saat katsottua komentorivi työkalulla. Asenna cinder työkalu ensin tietokoneellesi ja sen jälkeen aja komento

cinder quota-usage <tenant_id>

Vastauksena tulee sekä käyttöaste että rajoitukset, jotka ovat käytössä tilissäsi.

VIRTIO AJURIT

Windows updatesta löytyy tällä hetkellä valinnaisena päivityksenä SUSE:n QEMU/KVM jakeluille tehty virtio-ajuripäivitys. Päivitys löytyy ainakin Windows Server 2012 R2:lle. Microsoft jakelee tätä kaikille virtio-laitteille, vaikka tunnetusti virtio ajureissa, kuten monissa muissakin hypervisor kohtaisissa ajuri/tools paketeissa, on versioriippuvuuksia hypervisorin ja ajuriversion välillä. Kyseinen ajuripäivitys rikkoo Windowsin levyohjaimen ajurin ja tekee kyseisen instanssin käynnistämisestä mahdotonta!

Tätä ajuripäivitystä, kuten yleensä muitakaan tuntemattomia ajuripäivityksiä, ei missään nimessä tule asentaa palvelimiin. Varsinkin virtio-ajurien kohdalla on syytä ajaa vain testattua ja tuettua versiota ajureista ellei jonkin ongelmatilanne pakota toisin toimimaan.

Workaround ongelman kiertämiseen tilapäisesti, jotta palvelimen datoihin pääsee käsiksi:

1. Sammuta palvelin

2. Ota palvelimen snapshot

3. Odota, että snapshot valmistuu Image-palveluun

4. Aseta Images-palvelun (Glance) CLI-työkalulla juuri snapshotatulle imagelle IDE-emuloinnin pakotus levyohjaimelle:

    $ glance image-update –property hw_disk_bus=ide <snapshot imagen id>

5. Käynnistä uusi palvelin tällä imagella (luonnissa kestää hetki, kun uusi image ei ole hypervisorien cachessa vielä ja Windows image on kooltaan suhteellisen iso)

6. Uusi palvelin preparoi nyt automatic prepairit läpi, mutta valikosta voi valita “Exit and boot to OS”

7. Palvelin on nyt käynnissä IDE emuloidulla (hitaalla) levyllä ja mahdollista elvytystä kuten ajurien poistoa/rollbackkiä jne. voi yrittää

Lisäyksenä kohtien 6. ja 7. jälkeen. Jotain lisäpäivityksiä voi asentua vielä ensimmäisen”preparing automatic repair bootin” jälkeen. Palvelin käynnistyy vielä kerran. Hard reboot tämän jälkeen, palauttaa järjestelmän emuloituun IDE-moodiin. IDE-moodi on tosiaan melko hidas eli kärsivällisyyttä.

Muistattehan että järjestelmän varmuuskopiointi sekä ajantasainen palautussuunnitelma on erittäin tärkeä erilaisia vikatilanteita varten.

Alaotsikko: INCLOUD: ORKESTROINTI

Telian Cloud 9 orkestrointiominaisuuden avulla on mahdollista automatisoida palveluun tehtäviä resurssien lisäyksiä, muutoksia ja poistoja. Tämä helpottaa ja nopeuttaa huomattavasti varsinkin toistuvien toimenpiteiden suorittamista.

Lisättävät resurssit kuvataan orkestrointipohjaan. Orkestrointipohjan avulla voi muutamalla klikkauksella, jo muutamissa sekunneissa luoda palveluun kokonaisen ympäristön – verkot, reitittimet, instanssit, levytilan ja turvaryhmät. Orkestrointimoduuli tukee *OpenStack Heat* –orkestrointipohjien (HOT) lisäksi myös *Amazon Web Services CloudFormation* -pohjia.

Orkestrointipohjia voi lisätä palveluun suoraan Telia Pilven hallintapaneelista tai *Open Stack Heat* –rajapintaa käyttämällä.

Katso videomme siitä, kuinka orkestrointipohjien avulla luodaan täysin käyttövalmis WordPress-ympäristö. Video löytyy osoitteesta: https://www.youtube.com/watch?v=bAbWNWCGiC4

ORKESTROINTIPOHJA

Ohessa on kuvattu muutama esimerkki orkestrointipohjan syntaksista.

Esimerkiksi seuraavan pohjan avulla luodaan instanssi ja määritellään instanssin: palvelinkokoonpano *(flavor)*, levykuva *(image),* saatavuusalue *(availability zone)* sekä verkot, joihin instanssi liitetään.

Seuraavassa orkestrointipohjassa määritellään verkko:

OpenStack:in omaa ohjeistusta:

- Perusohje Heat-orkestrointipohjan tekemisestä: http://docs.openstack.org/developer/heat/template_guide/hot_guide.html
- Ohjeita eri OpenStack-resurssien syntakseista: http://docs.openstack.org/hot-reference/content/openstack-resource-types.html

ORKESTROINTIPOHJAN LISÄÄMINEN TELIA PILVI –HALLINTAPANEELISTA

Kirjaudu Cloud 9:n hallintapaneeliin ja klikkaa **Orchestration**. Valitse avautuvasta pudotusvalikosta **Stacks**.

Klikkaa avautuvalta sivulta **Launch stack**.

Seuraa uuteen ikkunaan avautuvan orkestrointipohjan lisäysvelhon ohjeita. Orkestrointipohjan lisäämisen jälkeen resurssit lisätään välittömästi palveluun.

Stacks-osiosta voi tämän jälkeen tarkastella ja hallita orkestrointipohjien avulla lisättyjä resursseja.

ORKESTROINTIPOHJAN LISÄÄMINEN OPENSTACK HEAT –RAJAPINTAA KÄYTTÄEN

Aloita asentamalla *Nova*-ohjelmisto. Löydät ohjeet verkkosivuiltamme seuraavasta ohjeartikkelista: Nova-ohjelmiston asennus

Asenna tämän jälkeen vielä *Heat*-ohjelmisto seuraavalla komennolla:

Windows

- *pip install python-heatclient*

Ubuntu, Debian, OS X

- *Sudo pip install python-heatclient*

Red Hat Enterprise Linux, CentOS, Fedora

- *Sudo python-pip install python-heatclient*

Esimerkkejä mm. orkestrointipohjan lisäämisessä käytettävistä komentorivikomennoista löydät täältä: http://docs.openstack.org/developer/heat/template_guide/environment.html

Alaotsikko: INCLOUD: SNAPSHOT

INSTANSSI SNAPSHOT (IMAGE)

Yksittäisestä instanssista voidaan ottaa snapshot, jota voidaan käyttää esimerkiksi uusien instanssien provisioinnnissa tai olemassa olevan instanssin uudelleenrakentamisessa.

Huomaathan, että snapshotteja ei kannata käyttää varmuuskopiona, sillä ne tallentuvat samalle fyysiselle laitteelle kuin missä lähdelevy on.
Siitä voi olla apua palautustilanteessa esim. inhimillisen virheen jälkeen, mutta ei fyysisen laitevian kohdatessa.

Snapshotit tulee ladata talteen muualle, mikäli niitä käytetään kuin varmuuskopioita.

Suosituksia ja huomioita

- Snapshot ei kuluta projektin quotaa eli niistä ei veloiteta lisähintaa.
- Snapshot ei saa koskaan korvata varsinaista varmuuskopiointia.
- Snapshot kannattaa luoda sammutetulle instanssille, että kaikki tiedostot on varmasti suljettu sekä kaikki kirjoitusoperaatiot suoritettu loppuun.
- Snapshotin aikana instanssi menee pause-tilaan, jonka takia instanssi voi tuntua olevan “jumissa” pidemmän aikaa. Instanssi ja sen käyttöjärjestelmä ei ole käytettävissä operaation aikana.
- Snapshot ei tallenna instanssin käyttömuistia (RAM) eli mahdollisesti käynnissä olevien sovellusten tallentamaton data menetetään mikäli instanssi on käynnissä snapshottia ottaessa.

- Snapshottia ei pysty peruuttamaan sen alettua eli operaation tulee antaa valmistua eikä snapshottia saa koettaa poistaa kesken operaation.

Snapshotin luominen ja palauttaminen

- Varaa operaatiolle noin 15-60 minuuttia ja sammuta instanssi käyttöjärjestelmätasolta
- Mene Cloud 9 hallintaan osoitteessa: https://control.nebulacloud.fi/
- Luo snapshot: Compute -> Instances -> [INSTANSSI] -> Actions: Create snapshot
- Odota snapshotin muodostumista seuraamalla sen tilaa images-listasta: Compute -> Images -> [SNAPSHOT] -> Status (Active = Valmis)
- Snapshotin valmistuttua sen voi palauttaa kahdella tavalla:
    - Olemassa olevan instanssin päälle (Rebuild from image) – Instanssin asetukset säilyvät ja juurilevyn data ylikirjoitetaan.
    - Uudeksi erilliseksi instanssiksi (Launch from image) – Instanssit asetukset joutuu määrittämään uudelleen, kuten uutta instanssia luodessa.
- Palautus olemassa olevan instanssin päälle: Compute -> Instances -> [INSTANSSI] -> Actions: Rebuild instance -> Select Image: [SNAPSHOT] -> Rebuild instance
- Palautus uudeksi erilliseksi instanssiksi: Compute -> Images -> [SNAPSHOT] -> Launch -> Täytä tarvittavat tiedot, kuten uutta instanssia luodessa -> Launch

VOLUME SNAPSHOT (SNAPSHOT)

Snapshot voidaan ottaa yksittäisestä volumesta. Volume snapshot ei vaikuta instanssin suorituskykyyn olennaisesti, volume snapshost tapahtuu alemmalla levyjärjestelmä tasolla.

Suosituksia ja huomioita

- Volume snaphost veloitetaa kuten normaali volume.
- Snapshot kannattaa ajaa sammutetulle instanssille, että kaikki tiedostot on varmasti suljettu sekä kaikki kirjoitusoperaatiot suoritettu loppuun.
- Vaihtoehtoisesti volumen voi irroittaa instanssista, kun se ei ole enää varattuna käyttöjärjestelmätasolla ja siitä voi muodostaa snapshotin ilman, että instanssia sammutetaan.

Snapshotin luominen ja palauttaminen

- Snapshotin muodostaminen kestää tyypillisesti muutaman minuutin.
- Sammuta instanssi käyttöjärjestelmätasolta.
- Mene Cloud 9 hallintaan osoitteessa: https://control.nebulacloud.fi/
- Irrota volume instanssista: Volumes -> Volumes -> [VOLUME] -> Actions: Manage attachments -> Detach volume

- Luo snapshot: Volumes -> Volumes -> [VOLUME] -> Actions: Create volume snapshot
- Odota snapshotin muodostumista seuraamalla sen tilaa snapshots-listasta: Volumes -> Snapshots -> [SNAPSHOT] -> Status (Available = Valmis)
- Palautus uudeksi volumeksi: Volumes -> Snapshots -> [SNAPSHOT] -> Actions: Create volume -> Create volume
- Liitä snapshotista luotu uusi volume instanssiin ja poista vanhan volumen snapshotit ja volume itse, mikäli niitä ei tarvita.
    - Uuden volumen liittäminen: Volumes -> Volumes -> [UUSI VOLUME] -> Actions: Manage attachments -> Valitse instanssi listasta -> Attach volume
    - Vanhan volumen poistaminen: Volumes -> Volumes -> [VANHA VOLUME] -> Snapshosts -> [JOKAINEN SNAPSHOT] -> Actions: Delete volume snapshot -> Kun kaikki volumen snapshotit on poistettu -> [VANHA VOLUME] -> Actions: Delete volume

Alaotsikko: INCLOUD: WINDOWS JA PCI

Useiden virtual PCI-laitteden Hot-Plug toiminta uudelleen käynnistyksen yhteydessä

Jossain tapauksissa on huomattu että Windows virtuaalikoneelta on tapahtunut seuraavia ongelmia sammutus ja uudelleen käynnistys yhteydessä.

- Jäänyt osa erillisistä volumeista ”Offline” tilaan Windowsissa
- Verkkointerfaceilta kadonnut staattinen IP-konfiguraatio

Kyseiset oireet saatiin rajattua siihen, että hot-plugina liitetyt laitteet päätyvät saamaan ennen ensimmäistä power cycleä ns. puhtaan PCI-osoitteen hypervisorilta. Pilvi kuitenkin hallitsee ja generoi hypervisoreille keskitetysti instanssien konfiguraatiota, eikä tätä tilapäistä osoitetta voida mihinkään heijastaa. Tämän seurauksena kun instanssi ensimmäisen kerran sammutetaan (shutdown) ja käynnistetään uudestaan (pelkkä reboot ei siis riitä tätä triggeröimään) loksahtaa device konfiguraatiosta sopivaan koloon ja näin ollen ei säilytä tuota PCI-osoitetta, joka sillä hot-plugin aikana oli.

Windows guestit bindaavat verkkokonfiguraationsa nimenomaan tiettyyn PCI-laitteeseen kohdistettuun interfaceen. Jos tämän PCI-laitteen numerointi muuttuu, ei Windows enää pidä sitä samana laitteena. Windows guestin osalta myös volumejen automaattinen löytäminen oli osittain samasta syystä kateissa, koska default asetuksilla Windows ei salli millään tapaa muuttuneiden ”SAN-levyjen” nousta Online tilaan automaattisesti (tarkoitettu suojafeatureksi jaettuun LUN-käyttöön).

Tästä ei synny haittaa esim. Linux käyttöjärjestelmissä (joissa useimmiten MAC-osoite, ajurin bindaus tms. mekaniikka hoitaa tuon) tai Windows konfiguraatioissa, joissa on käytössä 1kpl DHCP:llä varustettuja verkkoliityntöjä.

Fixes & workarounds:

- Windows voidaan konfiguroida sallimaan volumejen Onlinetys ja tunnistus siitä huolimatta, että PCI-osoite on heilahtanut. Komentamalla DISKPART:ssa ”san policy=OnlineAll” (http://www.happysysadm.com/2010/11/disk-is-offline-because-of-policy-set…). Tätä asetusta käyttäen Windows 2012 ja uudempiin guesteihin voi edelleen liittää tarvittaessa volumeita tarvittaessa hotplugina.
- Verkkoliitosten osalta Windows guestien tilanne on se, että kaikki verkkointerfacejen lisäykset suositellaan tehtäväksi instanssi sammutettuna. Tällä varmistut siitä, että konfiguraatiot interfaceen tehdään varmasti oikeaan PCI-osoitteeseen kohdistettuna eivätkä ne tulevaisuuden power cycleissä katoa.
- Kaikkiin käyttöönottotestauksiin ja vastaaviin testeihin olisi aina hyvä lisätä rebootin lisäksi (tai tilalle) myös shutdown + start testi, ainakin Pilvi 9.0:n osalta. Koska reboot operaatio tapahtuu saman prosessin sisällä, mutta shutdownin kautta instanssi oikeasti käynnistetään hypervisorilla uuteen prosessiin, nähdään tämän ns. power cyclen kautta helpommin tämän kaltaiset vikatilanteet jo ympäristön testauksessa.

Alaotsikko: INCLOUD: VOLUMEIDEN LISÄÄMINEN WINDOWS-INSTANSSEIHIN

Alla olevat toimenpiteet takaavat, että instanssiin liitetyt volumet ovat online-tilassa myös sen jälkeen, kun instanssi käynnistetään uudelleen. Tämä saattaa tapahtua esimerkiksi Pilvi 9.0 -alustan versio- tai tietoturvapäivityksissä.

Vaihtoehto 1:

Käynnistä DISKPART.EXE -työkalu ja anna seuraava komento:

san policy=OnlineAll

Vaihtoehto 2:

Liitä volume Windowsiin **ainoastaan silloin kun instanssi on sammutettuna**.

Ohje:

HUOM. VARMISTA ETTÄ LEVY EI OLE CLUSTER LEVY JA KÄYTÖSSÄ TOISELLA PALVELIMELLA.

Mitä tehdään kun Windows palvelimelta puuttuu levy (esim. D:).

Tarkistetaan

Start -> Run -> diskpart (Run as Administrator)

Kirjoitetaan *LIST DISK*

DISKPART> list disk

```
Disk ###  Status      Size     Free     Dyn  Gpt
--------  ----------  -------  -------  ---  ---
Disk 0    Online       119 GB      0 B
```

```
Disk 1    Offline        931 GB      0 B

DISKPART>
```

Kuten huomataan, niin Disk 1 on Offline. Jotta, levy saataisiin takaisin, täytyy komentaa

SELECT DISK 1 (valitaan DISK 1 aktiiviseksi mille toimenpiteitä suoritetaan).

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
DISKPART>
```

Varmistetaan että oikea levy on valittuna.

```
DISKPART> list disk

Disk ###  Status        Size     Free     Dyn  Gpt
--------  -------------  -------  -------  ---  ---
Disk 0    Online         119 GB      0 B
* Disk 1    Offline        931 GB      0 B

DISKPART>
```

Komennetaan levy ONLINE tilaan

```
DISKPART> online disk
DiskPart successfully onlined the selected disk.
DISKPART>
```

Tämän jälkeen voi varmistaa, että levy on oikeasti ONLINE

```
DISKPART> list disk

Disk ###  Status        Size     Free     Dyn  Gpt
--------  -------------  -------  -------  ---  ---
Disk 0    Online         119 GB      0 B
* Disk 1    Online         931 GB      0 B

DISKPART>
```

HUOM! Mikäli levy on kirjoitussuojattu, tulisi ajaa DISKPART kautta seuraava komento: *attributes disk clear readonly*

eli:

(oletuksena että disk 1 on se mikä oli Offline tilassa)

DISKPART> select disk 1
Disk 1 is now the selected disk.
DISKPART> attributes disk clear readonly
Disk attributes cleared successfully.
DISKPART>

Nyt levyn pitäisi toimia normaalisti.

Windows puolelta tuo pitäisi muuttaa DISKPART:illa käyttöön.

Nyt levyn pitäisi näkyä myös Explorerissa / Tiedostonhallinnassa. Suosittelemme palvelimen uudelleenkäynnistystä, jotta palvelut (SERVICES) jotka käyttävät näitä levy-resursseja käynnistyvät oikeinja löytävät datan.

Alaotsikko: INCLOUD: VPN/NAT -PIKAOHJE

Cloud 9 – VPN-yhteydet
Cloud 9-palvelussa VPN-yhteydet ovat sallittuja ja niitä ei ole erikseen estetty. VPN-yhteyden voi luoda asentamalla instanssiin tai instansseihin tarvittava VPN-ohjelmisto, tai asentaa erikseen appliance-paketin hoitamaan VPN-yhteyksiä. Esimerkissämme teemme ohjelmallisen VPN-yhteyden DMZ-palvelimen läpi (bastion host). Muut instanssit ovat ainoastaan LAN-verkossa.

HUOM! VPN-yhteyksissä on tärkeää sallia instanssin reitittämä liikenne ulkopuolisista verkoista, koska palvelussa on port security (antispoof) ominaisuus päällä. Bastion host-instanssi ei voi välittää liikennettä jos sitä ei erikseen sallita.

Luodaan esimerkkiä varten kaksi verkkoa, DMZ (10.0.0.0/24) ja LAN (10.1.0.0/24)

Asennetaan Cloud 9:ään Bastion host –instanssi Centos 7 tiny-flavorillä, tälle liitäntä kumpaankin verkkoon. Varataan Floating IP ja sidotaan se instanssin DMZ-porttiin.

Haetaan consolesta palvelimelle Openstack RC-tiedosto, tallennetaan tiedostoon pysyvästi OpenStack-salasana, ja ajetaan tiedosto (käsky ”*source tiedosto*”)

Asennetaan instanssiin Openstackin työkalut (RDO), pakettien nimet python-PROJECTclient (missä PROJECT on nova, neutron, cinder, swift yms)

Kun python-neutronclient on asennettu, käsketään
neutron port-list

Tuloste on jotakuinkin kuvanmukainen, ja tässä tapauksessa etsimme LAN-verkon porttia (esimerkissä IP 10.0.0.4, eli portin id on cbbb1c32-a516-4a11-a5ea-780e733dfc11)

Sallitaan tältä portilta liikennöinti LAN-verkosta ulospäin käyttäen mitä tahansa IP-osoitteita:
neutron port-update cbbb1c32-a516-4a11-a5ea-780e733dcf11 –allowed-address-pairs type=dict list=true ip_address=0.0.0.0/0
ip_address-tietueeseen voi toki laittaa tiukemman rajoituksen, jos on tiedossa että VPN:n läpi tulee tiedossa oleva rajatumpi verkko.

Nyt bastion host voi välittää liikennettä VPN-verkon ja LAN-verkon välillä.

VPN/NAT
Jos haluaa kaiken liikenteen ohjata oman NAT/VPN –instanssin läpi, reitittävällä instanssilla pitää linuxissa erikseen mahdollistaa tämä:

echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -o eth0 -A POSTROUTING -j MASQUERADE
iptables -t nat -o eth1 -A POSTROUTING -j MASQUERADE

Tämän jälkeen muut instanssit voivat käyttää tätä instanssia oletusyhdyskäytävänä, ja kyseisen LAN-verkon asetuksissa voi määritellä instanssin olemaan default gateway. Näin oikea gateway tulee automaattisesti.

HUOM! Älä määrittele MASQUERADE-sääntöä loopback-kortille (lo), tämä saattaa häiritä palvelimen sisäistä toimintaa. Lisäksi FORWARD-taulussa ei pidä estää liikennettä jos instanssi toimii reitittimenä / NAT-yhdyskäytävänä.

DHCP ja staattiset reitit
Jos halutaan että instansseilla tietty verkko reitittyy oletusyhdyskäytävän sijasta tiettyyn osoitteeseen (esim VPN-instanssille), tämän voi toteuttaa suoraan DHCP-ominaisuuksissa. Networks -> LAN -> Edit Subnet -> Next -> Host routes. Syntaksi on verkko/maski pilkku gateway (esim: 10.2.0.0/24,10.1.0.1). Tässä tapauksessa 10.1.0.1 on bastion hostin LAN-portin osoite.

VPN-ohjelmiston valinta
Jos tarve on vain kahden verkon yhdistäminen ja kummankin verkon rajalla on Linux-instanssi, VPN-yhteytenä voi käyttää esim OpenVPN SSL/TLS-yhteyttä:
http://openvpn.net/

Mikäli toisessa päässä on erillinen VPN-palomuuri tai -reititin, esim IPSec-yhteydet onnistuvat StrongSwan –ohjelmalla:
https://www.strongswan.org/

Lisäksi PPTP-pohjaisen yhteyden saa rakennettua Linuxiin melko helposti mutta emme suosittele sen käyttämistä.

STRONGSWAN-OHJE (IPSEC)

Esimerkkiä varten meillä on kaksi /24 verkkoa, DMZ ja LAN. CentOS 7-palvelimellamme on kaksi porttia:

DMZ: 10.0.0.1
LAN: 10.0.1.1

Testipalvelimella on myös Floating IP 77.86.179.250 joka on kiinnitetty DMZ-porttiin.

Toisessa kaupungissa sijaitsee VPN-palomuurireititin McAfee SG560 julkisessa IP-osoitteessa 9.9.9.9, ja tämän laitteen takana on toimiston LAN-verkko 10.10.0.0/24

Pilven Security Groupeissa palvelimelle pitää sallia IPSec-yhteyksiin tarvittavat portit ja protokollat VPN-laitteelta (UDP 500, UDP 4500, IP-protokolla 50 eli ESP)

VPN-palomuurin päässä IPSec-asetukset ovat:

Phase 1: IKEv1 3DES-SHA-DH5 (MODP1536)
Phase 2: 3DES-SHA-DH5 (MODP1536, PFS päällä)
PreShared key: testiavain123

VPN-yhteydessä Pilven pään StrongSwan on loogisesti ”left” ja vastapään VPN-laite ”right”, joten yhteyspisteet nimetään kummassakin päässä ID-tiedolla ”@left” ja ”@right”. ID-tietojen on täsmättävä, muuten yhteys ei muodostu.

Asennetaan StrongSwan testipalvelimeen:

yum install strongswan strongswan-libipsec

Asennuksen jälkeen kirjoitetaan /etc/strongswan/ hakemistoon seuraavat tiedostot:

ipsec.conf:

config setup conn
%default ikelifetime=60m keylife=20m rekeymargin=3m keyingtries=1 authby=secret keyexchange=ikev1 mobike=no conn net-net ike=3des-sha-modp1536 esp=3des-sha-modp1536 left=10.0.0.1 leftsubnet=10.0.1.0/24 leftid=@left leftfirewall=yes right=9.9.9.9 rightsubnet=10.10.0.0/24 rightid=@right auto=add

ipsec.secrets:

@left @right : PSK testiavain123

Muihin tiedostoihin ei tarvitse koskea.

Sitten käsketään:

strongswan start
strongswan up net-net

Yhteys muodostuu laitteiden välillä ja liikenne LAN-verkkojen välillä toimii kunhan ”*neutron port-update*” käskyllä liikenne LAN-portista on sallittu.

Jos haluat yhteyden nousevan palvelimen käynnistymisen yhteydessä, pitää strongswan laittaa bootissa käynnistymään käskyllä

systemctl enable strongswan.service

ja vaihtaa ipsec.conf-tiedostosta “auto=add” muotoon “auto=start”.

Käsky *strongswan up net-net* antaa seuraavankaltaisen tulosteen:

strongswan up net-net initiating Main Mode IKE_SA net-net[1] to 9.9.9.9 generating ID_PROT request 0 [SA V V V V] sending packet: from 10.0.0.1[500] to 9.9.9.9[500] (212 bytes) received packet: from 9.9.9.9[500] to 10.0.0.1[500] (136 bytes) parsed ID_PROT response 0 [SA V V V] received unknown vendor ID: 4f:45:49:70:42:4c:6d:5f:4e:5b:6f:59 received DPD vendor ID received NAT-T (RFC 3947) vendor ID generating ID_PROT request 0 [KE No NAT-D NAT-D] sending packet: from 10.0.0.1[500] to 9.9.9.9[500] (308 bytes) received packet: from 9.9.9.9[500] to 10.0.0.1[500] (292 bytes) parsed ID_PROT response 0 [KE No NAT-D NAT-D] local host is behind NAT, sending keep alives generating ID_PROT request 0 [ID HASH] sending packet: from 10.0.0.1[4500] to 9.9.9.9[4500] (68 bytes) received packet: from 9.9.9.9[4500] to 10.0.0.1[4500] (68 bytes) parsed ID_PROT response 0 [ID HASH] IKE_SA net-net[1] established between 10.0.0.1[left]...9.9.9.9[right] scheduling reauthentication in 3329s maximum IKE_SA lifetime 3509s generating QUICK_MODE request 208874606 [HASH SA No KE ID ID] sending packet: from 10.0.0.1[4500] to 9.9.9.9[4500] (372 bytes) received packet: from 9.9.9.9[4500] to 10.0.0.1[4500] (356 bytes) parsed QUICK_MODE response 208874606 [HASH SA No KE ID ID] CHILD_SA net-net{1} established with SPIs 67d15f15_i ec25c466_o and TS 10.0.1.0/24 === 10.10.0.0/24generating QUICK_MODE request 208874606 [HASH] sending packet: from 10.0.0.1[4500] to 9.9.9.9[4500] (60 bytes) connection 'net-net' established successfully

Alaotsikko: INCLOUD: MIGRAATIO INCLOUD 9 -PALVELUUN

Onko sovelluksesi hankala asentaa? Media hukassa? Tarvitset konsultin konfiguroimaan sovelluksesi? Voit siirtää nykyiset palvelimesi sellaisenaan Cloud 9-palveluun.

MIGRAATIOPALVELUT

Olit sitten tuomassa yhtä tai useampaa palvelinta, saat Telian asiantuntijoilta apua siirtämään nykyiset Windows- ja Linux-palvelimesi mutkattomasti.

OMAN LEVYKUVAN TUOMINEN

Cloud 9 virtualisoinnin moottorina on KVM teknologia. KVM virtualisointi tukee käytössä RAW ja QCOW2 levykuva formaatteja. Näitä levykuvia on mahdollista tuoda hyödyntäen selaimen hallintapaneelia, komentroriviltä tai API työkaluilla. Uuden palvelimen provisioinnin yhteydessä voit valita lähteeksi oman levykuvan ja siirtää sen verkon yli.

OLEMASSA OLEVAN PALVELIMEN SIIRTO VAI UUDEN PYSTYTYS?

Palvelin siirretään ”as-is” Pilveen

- Palvelimen käyttöjärjestelmä, sovellukset, tiedostot ja konfiguraatiot siirtyvät sellaisenaan.

- Suositellaan kun sovelluksen uudelleen asentaminen ja konfigurointi on vaikeaa/kallista

Asennetaan uusi palvelin asennetaan

- Sovellukset asennetaan uudestaan ja konfiguroidaan.
- Suositellaan, jos sovellus on kohtuullisella vaivalla asennettavissa
- Etuja ovat tuore käyttöjärjestelmä, ajurien toimivuus, tuoreet sovellukset

WINDOWS-PALVELINTEN MIGRAATIO

Windows-palvelinten migraatio suoritetaan tyypillisesti asentamalla uusi Windows-palvelin samalla patch tasolla oleva palvelin rinnalle Cloud 9-palveluun.

1.Windows-käyttöjärjestelmä provisioidaan pilveen ja asennetaan migraatiosovellus

2. Lähdepalvelimeen asennetaan sovellusagentti
3.”Patch” tason varmistetaan olevan sama.
4.Sovellusagentti kopioi taustalla lähdepalvelimesta tiedostot kohdepalvelimelle
5.Yliheitto käyttökatko
6.Palvelin käynnistetään ja toimivuus varmistetaan

Sovellusagentti kopio kohdejärjestelmän tiedostot blokkitasolla palvelimesta toiseen ja varmistaa että kaikki tiedostot ja konfiguraatiot ovat identtiset.

LINUX-PALVELINTEN MIGRAATIO

Linux-palvelimet siirrettään helpoiten ottamalla nykyinen tiedostojärjestelmä “pakettiin” konvertoimalla se toisella palvelimella QCOW muotoiseksi ja siirtämällä Cloud 9-palveluun.

1.Tiedostojärjestelmä ”paketoidaan” lähdepalvelimella
2.Paketti kopioidaan kohdepalvelimelle verkon yli
3.Paketti konvertoidaan QCOW levykuvaksi
4.Levykuva siirretään Telia Pilveen
5.Palvelin käynnistetään ja toimivuus varmistetaan

Alaotsikko: INCLOUD: NOVA-OHJELMISTON ASENNUS

Windows
Mene sivulle http://www.activestate.com/activepython/downloads

Valitse ladattavaksi versio joka on alle 3.x. Suositteleva versio on Python 2.7. Asenna Active-Python paketti tietokoneelle, avaa Windowsin komentorivi ja aja sieltä seuraavat komennot komentorivityökalun asentamiseksi:

pip install PBR
pip install python-novaclient

Linux (Ubuntu)
Aja seuraavat komennot:

sudo apt-get install python-pip
sudo pip install pbr
sudo pip install python-novaclient

Ympäristömuuttujien määrittely
Tämä ei ole pakollista, mutta tämän tekeminen helpottaa komentorivin käyttöä kun tietoja ei tarvitse määritellä erikseen jokaisen komennon yhteydessä. Saatte tarvittavat tiedot projektillenne Horizon-hallintapaneelin kautta seuraavasti:

- https://control.nebulacloud.fi/project/access_and_security/
- API Access
- Valitse DOWNLOAD OPENSTACK RC FILE
- Avaa tiedosto ja etsi sieltä 32-merkkinen OS_TENANT_ID

Windows-ympäristömuuttujat
Aja komentorivin kautta seuraavat komennot:

set OS_AUTH_URL=https://identity.fi-1.nebulacloud.fi:5000/v2.0
set OS_TENANT_ID=<TENANT_ID> set OS_USERNAME=<KÄYTTÄJÄTUNNUS>
set OS_PASSWORD=<SALASANA> set OS_REGION_NAME=fi-1

Linux-ympäristömuuttujat
Aja komentorivin kautta seuraavat komennot:

export OS_AUTH_URL=https://identity.fi-1.nebulacloud.fi:5000/v2.0
export OS_TENANT_ID=<TENANT_ID>
export OS_USERNAME=<KÄYTTÄJÄTUNNUS>
export OS_PASSWORD=<SALASANA>
export OS_REGION_NAME=fi-1

Testaa toimivuus
Voit varmistaa Novan komentorivityökalun toiminnan esimerkiksi kokeilemalla kaikkien projektisi palvelinten listausta seuraavasti:

nova list

Jos työkalun asennus on mennyt onnistuneesti, palautuu komennolla listaus projektin palvelimista.

Muiden komentorivityökalujen (Glance, Cinder…) asennuksesta löydät tietoa OpenStackin omasta dokumentaatiosta:

- https://docs.openstack.org/newton/user-guide/common/cli-install-openstack-command-line-clients.html

Alaotsikko: INCLOUD: DOCKERIT

Dockerit on uusi tapa ajaa sovelluksia omissa ympäristöissään, “containers”. Dockereiden suurin etu on niiden sisällä olevien sovellusten siirrettävyys alustalta tai arkkitehtuurilta toiseen, ilman että niiden alla olevaan käyttöjärjestelmään tai palvelimeen tarvitsee sovelluksen kannalta juurikaan kiinnittää huomiota. Tämä vähentää turhaan käyttöjärjestelmien kanssa pelaamiseen käytettyä aikaa ja vapauttaa resursseja itse tekemiseen.

Toinen loistava ominaisuus on kaikille yhtenäinen ympäristö. Esimerkiksi softakehittäjät voivat koodata omalla läppärillään sovellusta containereihin, joiden ympäristö on identtinen pilvessä pyörivän tuotannon kanssa.

Yllä oleva kuva havainnollistaa, miten Dockerien käyttö voi merkittävästi vähentää ylläpidettävien käyttöjärjestelmien (Guest OS) määrää ympäristössä. Tämä helpottaa ylläpitoa ja luo joustavuutta kehittäjille.

Moniin tavanomaisiin teknologioihin ja sovelluksiin löytyy valmiita pohjia Dockerhubista. Oman Docker imagen voi luoda tekemällä määrittelytiedoston, eli Dockerfilen. Dockerfilessä kuvataan mitä ominaisuuksia, sovelluksia ja esivalmisteluja imageen halutaan viedä itse sovelluksen suorittamista varten.

Dockerfilejä on helppo versio hallita esim. Gitillä, jolloin konfiguraatiosta säilyy automaattisesti historiatieto. Kuinka moni muistaa miettineensä, että mitenkäs sitä 3 vuotta sitten asennettiin se epästandardi versio jostain laajennuksesta, kun sovelluksen kehitystiimi sitä vaati?

Seuraavassa esimerkissä luodaan yksinkertainen Docker image, jossa pyörii Nginx webpalvelin. Tätä varten Dockerfile tiedostoon määritellään seuraavat parametrit:

FROM centos:centos7 RUN yum install epel-release -y RUN yum update -y && yum install nginx -y ADD run.sh /run.sh RUN sed -i ‘1 i\daemon off;’ /etc/nginx/nginx.conf RUN chmod +x /run.sh EXPOSE 80 ENTRYPOINT /run.sh

Kyseessä on hyvin yksinkertainen konfiguraatio, joka hakee pohjaimageksi CentOS 7 ympäristön ja ajaa siihen viimeisimmät tietoturvapäivitykset sekä asentaa Nginx-palvelimen omasta RPM-repositorysta. Lopuksi imageen lisätään tiedosto, jolla nginx saadaan käynnistymään aina, kun docker luodaan imagesta. Asetamme sen myös käynnistymään suoraan prosessina run.sh scriptiä kutsuttaessa. Tiedostossa määritellään myös missä portissa luotu docker kuuntelee, kun se on käynnissä.

run.sh sisältää vain komennon jolla nginx käynnistetään.

#!/bin/bash /usr/sbin/nginx

Tallenna tiedosto nimellä run.sh

Nyt kun määritys imagea varten on valmis haluamme saada sen ajoon. Luomme tätä varten Telian Cloud 9:aan instanssin, jossa voimme ajaa Dockereita. Haluamme myös esikonfiguroida User dataa hyväksikäyttäen virtuaalipalvelimen suoraan valmiiksi Dockeriamme varten. Tätä varten käytämme cloud-init ohjelmaa. Se on asennettu valmiiksi kaikkiin Telian tarjoamiin imageihin. Konfiguraatio on äärimmäisen helppo ja yksinkertainen:

#cloud-config timezone: Europe/Helsinki package_upgrade: true packages: – docker

runcmd: – [systemctl, enable, docker.service] – [systemctl, start , docker.service]

Kerromme cloud-config datalla instanssille, että haluamme aikavyöhykkeeksi Helsingin, päivittää kaikki paketit viimeisimpään versioon, sekä asentaa Docker-palvelimen riippuvuuksineen. Lopuksi vielä Docker service aktivoidaan ja käynnistetään. Huomaa, että esimerkin ”runcmd” osuus on systemd:lle, joka on käytössä esim. CentOS/RHEL7 jakeluissa. Ubuntulle ja Debianille löytyy omat työkalut serviceiden hallintaan. User-data luetaan, kun instanssi käynnistyy ja cloud-init noutaa metadatan itselleen työstettäväksi.

User datan voi antaa API:n, CLI-työkalujen tai käyttöliittymän kautta “userdata” kenttään:

Kun instanssi on käynnistynyt ja cloud-init suorittanut sille annetut tehtävät, voimme varmistaa, että instanssi on valmis tarjoilemaan docker containereita:

docker ps -a CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES

Meillä on nyt kaksi tiedostoa, Dockerfile sekä run.sh. Luomme näistä imagen josta voimme laittaa dockerin ajoon:

docker build –t nginx .

…

Kun image on valmis käynnistetään docker.

docker images REPOSITORY TAG IMAGE ID CREATED VIRTUAL SIZE nginx latest 66c461df60d9 28 seconds ago 323.5 MB centos centos7 34943839435d 2 weeks ago 224 MB # docker run -t -i -d -p 80:80 –name www nginx # docker ps CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES aedc1cc8f240 nginx:latest “/bin/sh -c /run.sh 1 seconds ago Up 1 seconds 0.0.0.0:80->80/tcp www

nginx on nyt omassa docker containerissaan ajossa ja siihen voidaan yhdistää instanssin julkiosoitteella:

Esimerkki on hyvin yksinkertainen ja se tarkoitus on näyttää miten Telian OpenStack-pohjaisen Cloud 9-palvelussa voidaan ajaa Dockereita. Isoissa Docker-ympäristöissä suosittelemme tutustumaan CoreOS käyttöjärjestelmään. Kyseisen käyttöjärjestelmän hallinnointi ja käyttöönotto on suhteellisen helppoa ja se sisältää mm. HA-ominaisuudet dockereiden ajamiseen. Lisäksi siitä löytyy suoraan image OpenStackissa käytettäväksi.

Alaotsikko: INCLOUD: KONSOLIYHTEYS

KONSOLIYHTEYDEN MUODOSTAMINEN PALVELIMELLE

Pilvi 9.0 palvelu tukee yhteyden muodostamista palvelimen konsolille joka vastaa pääsyä fyysiseen näppäimistöön / hiireen. Yhteys muodostetaan hyödyntäen VNC yhteyttä.

Vaatimukset

- HTML5 yhteensopiva selain
- Javascript

Lue teknologiasta VNC

Jos konsoli ei aukea

- Varmista että portti 6080 on auki ulospäin
- Tyhjänne selaimen cache tai käytä selaimen private/incognito tilaa.

Jos näppäimistösi toimii US muodossa

- Yleinen käytöntö etähallinnoissa on, että default locale fallback US koska muuten ongelmia olisi sellaisten alustojen kanssa, jotka eivät muuhun pysty. Suoraan ei voida myöskään päätellä mistä maasta ja millä näppäimistöllä loppukäyttäjäpalvelua käyttää. Ratkaisu siihen taas on sama kuten kaikissa iDRACeissa ja HP Iloissa ja muissakin etähallintakorteista
    - Vaihda käyttöjärjestelmästä ko. ikkunan keymap US:ksi.
    - Windowsissa Language Barista helpointa vaihtaa. Monissa Linux windows managereissa on myös mahdollisuus vastaavanlainen Language Bar asettaa käyttöön.
- Erikoismerkit voit tehdä kiertäen tämän sivun ALT koodien+ohjeiden mukaan http://tools.oratory.com/altcodes.html

Alaotsikko: INCLOUD: KÄYTTÖESIMERKKEJÄ

1. YKSITTÄINEN PALVELIN

Esimerkissä luodaan yksittäinen LAMP-palvelin (Linux with Apache, MySQL and PHP) websivun ylläpitoon.Tätä varten täytyy luoda:

- SSH-avain
- Verkko ja aliverkko
- Reititin, reitittimeen portti ja yhdyskäytävä
- Turvallisuusasetukset (Security Group)

- Palvelin (Instance)
- Julkinen IP-osoite (Floating IP)

Nämä toiminnallisuudet voidaan luoda palvelun hallintapaneelissa.

1.1. SSH-AVAIN

Palvelun käyttö aloitetaan luomalla SSH-avain, jolla palvelimille kirjaudutaan. Avain tulee ladata talteen ja tallettaa turvallisesti. **Huom! Avainta ei tallenneta Telia Pilveen, joten emme pysty palauttamaan sitä!** Pääset luomaan avaimen navigoimalla valikossa *Compute > Access & Security > Key Pairs*.

Esimerkissä luodaan avain *testkey* ja ladataan se työasemalle talteen.

1.2. VERKKO

Tässä kappaleessa ohjeistetaan verkon luominen, jos et halua käyttää sinulle luotuja oletusverkkoja.

Palvelinta varten tarvitaan myös verkko, jotka pääsee luomaan valikosta *Network > Networks > Create Network*.

Testiverkon nimi esimerkissä on *testnetwork*, verkossa *testsubnet* jonka avaruus on *10.0.0.0/24*. Käytä tässä vain sisäverkon IP-osoitteita käyttäviä verkkoja, julkiset IP-osoitteet allokoidaan muualla.

Yhdyskäytävänä voidaan käyttää esim. verkon viimeistä vapaata, eli verkkoblokin toiseksi viimeistä osoitetta. (Huomaathan, että verkon viimeistä osoitetta ei voi käyttää, sillä se on varattu verkon broadcast-osoitteeksi).

Nimipalvelimina voit käyttää nimipalvelimiamme (*217.30.180.230* ja *217.30.182.230*, kumpikin omalle rivilleen). Lopuksi tallenna verkon asetukset klikkaamalla C*reate*.

1.3. REITITIN

Tässä kappaleessa ohjeistetaan reitittimen luominen, jos et halua käyttää sinulle luotuja oletusreitittimiä.

Edellisessä vaiheessa loimme palvelinta varten sisäverkon, joka ei ole vielä yhteydessä ulkomaailmaan.

Yhteyden luominen aloitetaan luomalla ensin virtuaalinen reititin. Tämä löytyy valikosta *Network > Routers > Create Router.*

Esimerkissä reitittimen nimeksi annetaan *testrouter*. Tallenna, ja klikkaa sen jälkeen reitittimen nimeä listassa. Yhteys reitittimelle lisätään klikkaamalla *Add Interface* ja alasvetovalikosta valitaan aiemmin luotu *testsubnet*. Tälle reitittimelle annetaan ip-osoitteeksi testsubnetille määritelty yhdyskäytävä eli *10.0.0.254* ja tallennetaan klikkaamalla *Add interface*.

Oman verkkosi topologian voit nähdä navigoimalla *Network > Network Topology.* Tässä vaiheessa topologiasta näkee, että käytössä on verkko *testsubnet* joka on liitettynä reitittimeen, jolla ei vielä ole muita yhteyksiä.

Internetyhteys reitittimelle luodaan valikossa*Network > Routers > Set Gateway.* Valitse verkolle Availability Zone (sijainti), tässä esimerkissä *helsinki-1*. Verkon sijainti täytyy muistaa myöhemmin palvelinta luotaessa, joten kannattaa laittaa tämä muistiin.

Tämän jälkeen topologia näyttää, että reitittimellä on yhteys kahteen verkkoon, *testsubnet* ja *helsinki-1*.

1.4. TURVALLISUUSASETUKSET (SECURITY GROUP)

Ennen palvelimen luomista tulee varmistaa että palvelimelle voidaan ottaa SSH-yhteys. Turvallisuusasetukset löytyvät valikosta *Compute > Access & Security > Security Groups.* Turvallisuusasetuksissa voidaan luoda erilaisia sääntöryhmiä, joilla voidaan hallita palveluun luotujen palvelimien pääsyoikeuksia. Sääntöryhmät ovat palvelussa nimellä *Security Group*. Oletuksena on yksi sääntöryhmä, *default security group*, joka sallii liikenteen kaikkien kyseisessä ryhmässä olevien palvelimien kesken.

Esimerkissä luodaan uusi sääntöryhmä, ja nimetään se nimellä *testsecuritygroup*. Sääntöjä pääsee muokkaamaan klikkaamalla *Manage Rules*. **Huomaathan, että palveluun voi luoda vain rajallisen määrän sääntöryhmiä. Mikäli raja täyttyy, uusia sääntöryhmiä ei voi luoda.**

SSH-pääsyn voi sallia valitsemalla alasvetovalikosta vaihtoehdon SSH. Valitsemalla liikenteen lähteen voi valita, onko SSH-yhteys auki ulkoverkkoon, vai ainoastaan palveluun luodusta sisäverkosta.

Tässä esimerkissä SSH-pääsy avataan kaikkialta, eli lähde-IP -osoitteeksi määritellään *0.0.0.0/0* CIDR-kohtaan.

Sivustolle halutaan pääsy myös HTTPS-portista, joten seuraavaksi luodaan uusi sääntö jossa alasvetovalikosta valitaan HTTPS (443) ja lähdeosoitteeksi jälleen 0.0.0.0/0 CIDR-kohtaan. Tuloksena sääntölista näyttää tältä:

1.5. PALVELIMEN LUOMINEN

Seuraavaksi pääsemme luomaan palvelimen, valikosta *Compute > Instances,* klikkaamalla *Launch Instance*.

Ensin valitaan saatavuusalue (Availability Zone) jossa verkkomme sijaitsee, tässä tapauksessa siis *helsinki-1*. Palvelimelle tulee myös antaa nimi, tässä esimerkissä *testserver*.

Seuraavaksi valitaan palvelimen konfiguraatio, OpenStackissa nimitys *Flavor*. Tässä esimerkissä palvelimen konfiguraatioksi valitaan *nbl-n1-tiny* eli 40GB levytilaa, 1 VCPU ja 1024MB muistia.

Luotavien palvelimien määrä määritellään kohdassa *Instance Count*, tässä tapauksessa luodaan vain yksi palvelin. Valitaan palvelimen käynnistyslevykuva (*Boot source image*), käytännössä siis valitaan millä käyttöjärjestelmällä palvelin halutaan luoda. Tässä esimerkissä käyttöjärjestelmäksi valittiin CentOS7.

Seuraavaksi tarkistetaan muut palvelimen asetukset:

Access & Security -välilehdellä valitaan palvelimen luomiseen haluttu avainpari, tässä tapauksessa avainpareja on vain yksi, alussa luotu *testkey*. Tässä vaiheessa myös valitaan palvelimeen sovellettavat turvallisuusasetukset, eli valitaan sääntöryhmä *testsecuritygroup* listasta.

Verkko- välilehdellä on valmiiksi valittuna aiemmin luotu *testnetwork*:

Post-Creation -toimintoa voidaan käyttää sellaisten toimintojen käyttämiseen, jotka halutaan ajaa palvelimella käynnistyksen jälkeen. Esimerkkinä, tätä voi käyttää palvelimen päivittämiseen ennen varsinaista käyttöönottoa komennolla *yum -y update*.

Advanced Options voidaan käyttää levyn manuaaliseen partitioimiseen. Mikäli asetuksia ei tässä muuteta, levy partitioidaan automaattisesti.

Luo lopuksi palvelin klikkaamalla *Launch.*

1.6. JULKINEN IP-OSOITE (FLOATING IP)

Palvelimen luomisen jälkeen meillä on CentOS7 -palvelin IP-osoitteessa *10.0.0.1.* Palvelimen rakentumisen ja alkutoimintojen jälkeen palvelin näkyy listassa tilassa Status *Active*, Power State *Running*.

Jotta palvelimelle saisi pääsyn ulkoverkosta, sille pitää allokoida julkinen IP-osoite. IP-osoite allokoidaan valitsemalla valikosta *Associate Floating IP*. IP-osoite varataan klikkaamalla Plus-merkkiä ja valitsemalla sitten alasvetovalikosta verkkoavaruus (*helsinki-1)*.

Varattu IP-osoite pitää vielä liittää palvelimeen, valitaan alasvetovalikosta palvelimen portti jonka kautta halutaan reitittää liikenne. Tässä tapauksessa portteja on vain yksi, *testserver: 10.0.0.1*). Tämä ulkoinen ip-osoite ohjaa vain tähän sisäverkon porttiin (one-to-one NAT), eli sitä ei voida käyttää liikennöitäessä muihin portteihin palvelimella. Tallennuksen jälkeen tällä ip-osoitteella pääsee ulkoverkosta *testserver* -palvelimelle.

1.7. SSH-YHTEYS PALVELIMELLE

SSH-yhteyden palvelimelle voi luoda millä tahansa SSH-yhteysohjelmalla. Palvelimen nimenä käytetään palvelimen julkista ip-osoitetta, ja palvelimelle pääsy edellyttää alussa luotua SSH-avainta (*testkey.pem)*.

Käyttäjänimi on *centos*, *root* -kirjautuminen on oletuksena estetty (suositeltavampaa on käyttää *sudo* -komentoa).

$ ssh -i testkey.pem centos@77.86.179.5

HUOM! Jos käytät PuTTYa palvelimelle kirjautumiseen, muunna avaintiedosto PuTTY-formaattiin puttygen.exe -ohjelmistolla!

2. USEAMMAN PALVELIMEN KOKOONPANO

2.1. SETUP

Aiempaa esimerkkiä laajentaen voidaan tehdä useamman palvelimen kokoonpanoja. Tässä esimerkkinä käytetään web-palvelinta sekä siihen liitettyä tietokantapalvelinta, mutta samaa periaatetta noudattaen voidaan lisätä mitä tahansa palvelimia kokoonpanoon.

Kokoonpano:

- Kaksi verkkoa
- Kaksi aliverkkoa
- Kaksi reititintä
- Kaksi sääntöryhmää (security groups)
- Kaksi palvelinta

Aloita luomalla SSH-avain. Voit myös käyttää aiemmin luotua avainta.

Luo kaksi erillistä sisäverkkoa: DMZ ja sisäinen verkko.

- 10.0.0.0/24 (DMZ)
- 10.1.0.0/24 (internal)

Luo reititin, jolla on portti DMZ-verkkoon, ja ulkoinen yhteys *helsinki-1* -verkkoon.

Luo toinen reititin, ja sille kaksi porttia, yksi portti kumpaankin sisäverkkoon.

Luo sääntöryhmä joka sallii SSH- ja HTTP -yhteyden.

Luo toinen sääntöryhmä, joka sallii SSH- ja MySQL-yhteyden.

Luo *web-palvelin* ja liitä se DMZ-verkkoon.

Varaa ulkoinen IP-osoite, ja liitä se web-palvelimeen.

Luo *tietokantapalvelin* ja liitä se sisäiseen verkkoon.

2.2. YHTEENVETO

Kokoonpanossa on nyt web-palvelin joka toimii edustakoneena ja siihen saa otettua yhteyden SSH:lla, josta voi ottaa yhteyden edelleen tietokantapalvelimeen. Tietokantapalvelimella on pääsy

ulkomaailmaan vain, jos konfiguroit sisäiselle reitittimelle reitin osoitteeseen 0.0.0.0/0 DMZ-reitittimen kautta. Aliverkot ovat erillisiä ja kumpikin suojattu omien pääsyasetustensa kautta.

3. VIKASIETOINEN JÄRJESTELMÄ KUORMANTASAUKSELLA

Edellistä kokoonpanoa laajentamalla on mahdollista rakentaa monimutkaisiakin järjestelmiä, kuten korkean saatavuuden järjestelmiä kuormantasauksella.

Parhaiden käytäntöjen mukaan ei pitäisi milloinkaan olla riippuvainen yhdestä fyysisestä sijainnista (Tässä tapauksessa saatavuusalue, Availability Zone).

Tässä esimerkissä on käytössä

- Kaksi saatavuusaluetta
- Useita verkkoja
- Useita aliverkkoja
- Useita reitittimiä
- Useita sääntöryhmiä
- Useita julkisia ip-osoitteita
- 16 palvelinta, kummassakin saatavuusalueessa 8

Aloita luomalla SSH-avain. Voit myös käyttää aiemmin luotua avainta.

Luo kumpaakin saatavuusaluetta varten oma, erillinen DMZ-verkkonsa.

- AZ1: Helsinki-1DMZ 10.0.0.0/24
- AZ2: Helsinki-2DMZ 10.1.0.0/24

Luo kaksi erillistä sisäverkkoa kumpaankin saatavuusalueeseen.

- AZ1 Internal web 10.10.0.0/24
- AZ2 Internal web 10.11.0.0/24
- AZ1 Internal db 10.10.1.0/24
- AZ2 Internal db 10.11.1.0/24

Luo kumpaankin saatavuusalueeseen oma reitittimensä ja liitä ne omiin DMZ-verkkoihinsa. Aseta yhdyskäytäväksi saatavuusalueen oma yhdyskäytävä (**Public-Helsinki-1 ja Public-Helsinki-2)**

Luo kummallekin saatavuusalueelle toinen reititin, yhdistä se saatavuusalueen omaan DMZ-verkkoon ja *internal web* -verkkoon.

Luo kolmas reititin kumpaankin saatavuusalueeseen, jolla luodaan yhteys *internal db* – verkkoon.

Luo kaksi edusta/kirjautumispalvelinta, kummallekin saatavuusalueelle omansa. Nämä luodaan puhtaasti ylläpitotarkoituksiin. Liitä julkinen IP-osoite näihin koneisiin. Liitä palvelimiin sääntöryhmä jossa vain SSH on sallittu, niin että lähde-IP -osoite on vain ne osoitteet joista tiedät tarvitsevasi pääsyä palvelimille.

Luo kaksi web-kuormantasaajaa, kummallekin saatavuusalueelle omansa. Käytä sääntöryhmiä jotka sallivat vain portit HTTP ja/tai HTTPS osoitteesta 0.0.0.0/0 (kaikkialta), ja SSH vain edustapalvelimen sääntöryhmästä. Allokoi kummallekin palvelimelle oma ulkoinen IP-osoitteensa.

Luo web-palvelin haluamasi ominaisuuksilla, ja liitä se *internal web* -verkkoon. Käytä sääntöryhmää joka salllii vain HTTP- ja SSH -pääsyn. Valmistele palvelin tuotantovalmiiksi. Kloonaa palvelin ja luo yhteensä kuusi kopiota palvelimesta, niin että kummallakin saatavuusalueella on kolme.

Luo kaksi tietokanta-kuormantasaajaa*,* kummallekin saatavuusalueelle omansa. Käytä saman saatavuusalueen *internal db* -verkkoa. Sääntöryhmässä sallitaan pääsy ainoastaan web-aliverkoista, ja SSH DMZ-verkosta.

Luo tietokantapalvelin, liitä se *internal db* -verkkoon. Käytä sääntöryhmää joka sallii pääsyn SSH:lla DMZ-verkosta, ja tietokantaliikenteen sisäisestä web-verkosta.Luo klusterointi tietokantapalvelinten välillä haluamallasi tavalla.

Luo Object Storage -kansio, muuta se julkiseksi ja julkaise siellä kaikki sivuston staattinen sisältö.

Kuormantasausvaihtoehtoja on erilaisia järjestelmän sisällä. Molemmat saatavuusalueet voidaan pitää aktiivisena, tai toinen aktiivisena ja toinen valmiustilassa, sisältäen ajantasaisen tietokannan. Voit myös tasata kuormaa eri saatavuusalueiden välillä.

3.1. YHTEENVETO

Kokoonpanossa on nyt vikasietoinen ympäristö kahdennetulla kuormantasaajalla. Voit laajentaa sitä luomalla lisää palvelimia ja/tai kuormantasaajia.

Kummallakin saatavuusalueella on kaksi julkista IP-osoitetta; yksi hallintaan, ja toinen sivustoa varten.

Object Storea käyttäen voit käyttää samaa staattista sisältöä molemmista saatavuusalueista riippumatta siitä, kummalla saatavuusalueella sivusto sijaitsee.

Voit valvoa järjestelmän toimintaa edustapalvelimilta tai kuormantasaajilta, ja halutessasi käyttää API-rajapintaa järjestelmän skaalaamiseen.

REFERENSSIARKKITEHTUURIT

INcloud 9 tarjoaa helpon tavan esimerkiksi seuraaviin tarpeisiin

- hajauttaa palvelut maantieteellisesti
- suojata verkko segmentoimalla
- automatisoida infrastruktuurin provisiointi
- nopea ympäristön skaalaaminen

Arkkitehtuurin puolesta INcloud 9 tarjoaa asiakkaalle käytännössä vapaat kädet muokata arkkitehtuuristaan haluamansa kaltainen ja tässä dokumentissa on esitelty tyypillisesti kysyttyihin tarpeisiin ratkaisuja esimerkinomaisesti. Usein asiakkaalla onkin tarve yhdistellä eri vaihtoehtoja. Juuri tähän INcloud 9 on parhaimmillaan sen erinomaisen joustavuuden ansiosta.

Lataa PDF-dokumentti jossa käymme läpi seuraavat skenaariot

- Web hosting
- Web hosting kahdella saatavuusalueella
- Web hosting kuormantasauksella
- INcloud 9 osaksi toimistoverkkoa
- INcloud 9 turvalliset yhteydet muihin palvelimiin Telialla

Alaotsikko: INCLOUD: USEIN KYSYTYT KYSYMYKSET (UKK)

LASKUTUS

MIKSI IP-OSOITE MAKSAA VÄLILLÄ 4,80€ JA VÄLILLÄ 5,16€ /KK VAIKKA HINNASTOSSA LUKEE 5€? MYÖS WINDOWS-KÄYTTÖOIKEUDEN HINTA VAIHTELEE HIEMAN KUUKAUDESTA TOISEEN?

IP-osoitteet ja Windows käyttöoikeudet laskutetaan toteutuneiden minuuttien mukaan. Päivien määrä kuukaudessa vaihtelee, joten sitä kautta myös minuuttien määrä vaihtelee. Hinnaston hinta on laskettu 30 päivän mukaan. Tämä on kuvattu hintaliitteessä.

VOISINKO OSTAA PREPAID MALLILLA MYÖS WINDOWS-KÄYTTÖOIKEUDET JA IP-OSOITTEET, JOTTA EN SAISI JOKA KUUKAUSI LASKUA?

Toistaiseksi tämä ei ole mahdollista.

MITEN VOIN HALLINTA PREPAID TILAUKSIA?

Tilauksia hallitaan MyNebulasta.

MISTÄ NÄEN MITKÄ PREPAID PALVELIMET OVAT KÄYTÖSSÄ JA MITKÄ OVAT VAPAANA?

Prepaid tilauksia voitte hallinoida my.nebula.fi sivuston kautta, mistä näkee mitkä prepaid tilaukset ovat voimassa. Vastaavasti palvelimet näkyvät control.nebulacloud.fi sivuston kautta – vertaamaalla käytössä olevia palvelimia ja voimassa olevia tilauksia näkee mitkä tilaukset ovat käytössä ja mitkä vapaana.

MIKSI OLEN SAANUT LASKUN SEKÄ ON-DEMAND ETTÄ PREPAID PALVELIMISTA, KÄYTÖSSÄNI ON MIELESTÄNI VAIN PREPAID PALVELIMIA.

Todennäköisesti kyseessä on tilanne jossa valittu Prepaid palvelin ja käytössä oleva palvelin ovat tyypiltään erilaiset. Prepaid palvelin on varaus tiettyyn palvelintyyppiin, on se käytössä tai ei. On-Demand taas veloitetaan niiltä minuuteilta kun sopivaa Prepaid palvelinta ei ole varattuna käyttöön.

MIKÄ ON ON-DEMAND VERKKO LASKURIVI?

On-Demand verkko laskurivi sisältää julkisten IP-osoitteiden käyttökustannukset. Veloitus perustuu käytettyihin IP-osoite minuutteihin. IP-osoitteen kuukausihinta perustuu 30 päivän oletukseen eli 43 200 minuuttia/kk. Jos IP-osoitteita on enemmän/vähemmän ja/tai kuukauden päivien määrä vaihtelee niin veloitukset joustavat vastaavasti.

MITÄ TARKOITTAA PREPAID SOPIMUKSELLISESTI/KAUPALLISESTI?

Prepaid on käyttöoikeus resurssiin, kuten palvelimeen. Prepaidin sitovan määräaikaisuuden myötä asiakas saa merkittäviä säästöjä. Optimoimalla prepaid resursseja asiakas voi säästää jopa 67% kokonaiskustannuksista. Huomattavaa on että tämä käyttöoikeus veloitetaan asiakkaalta, riippumatta siitä onko palvelua käytetty ja että prepaid tilausta ei voi vaihtaa toiseen käyttöoikeuteen kesken sopimuskauden.

Analogia Prepaid-mallissa on kuin leasing autossa. Autosta veloitetaan kuukausimaksu käytti sitä tai ei. Sitä ei voi kesken sopimuskauden vaihtaa toiseen. Jos käyttöä on, se on huomattavasti edullisempi kuin taksi jossa ei ole kiinteitä kustannuksia.

ONKO MAHDOLLISTA SAADA RAPORTTIA KUSTANNUKSISTA PALVELIMITTAIN?

Cloud 9 laskutuslogiikka ei ole millään tavoin sidottu tiettyyn palvelimeen. Teknisesti palvelussa mitataan palvelimista ja levytilasta käyttöminuutteja, joista vähennetään mahdolliset prepaid varaukset. Tässä laskennassa ei kulje mukana tietoa mistää ulospäin näkyvistä palvelinnimistä, vaan ainoastaan sisäisiä tunnisteita. Samaten prepaid varaukset ovat kelluvia, eikä kohdistu tiettyyn yksittäiseen palvelimeen. Tämän takia laskutusaineistosta ei voida päätellä miten paljon mikäkin palvelin on maksanut laskutuskauden aikana.

Esimerkki

- Käytössä 2 kpl NBL-N1-Large
    - Toinen on käytössä koko kuukauden
    - Toinen on käytössä osan aikaa
- On-Demand käyttö NBL-N1-Large 70 000 MIN 1.1-30.9.2018
- Prepaid varaus NBL-N1-Large (43200min)
- Veloitetaan
    - NBL-N1-Large Prepaid
    - 26 800min * (241,92€/43 200min)

Toisekseen yllä mainitun kaltaisessa raportoinnissa olisi hyvin hankala kuvata selkeästi esimerkiksi levy-alueita jotka ovat olleet vain muutaman päivän keskellä kuukautta ajossa. Tämän takia laskulle on tiivistetty resurssien käyttö, sitomatta niitä esimerkiksi tekniseen palvelimeen tai levytilaan.

LASKUTUSESIMERKKI

Esimerkissä käymme läpi miten On-Demand ja Prepaid-veloitukset tapahtuvat käytännössä ja miten joustavaa On-Demand hinnoittelua voidaan hyödyntää lyhyissä tarpeissa.

Laskutusperiaatteet ovat kuvattu tarkemmin Telia Cloud 9 hinnastossa.

Tekninen toteutus

Normaalisti palvelinympäristö sisältää 3kpl NBL-HM1-LARGE palvelinta sekä 2000 Gt SSD-levytilaa näihin liitettynä. Palvelimet ovat hankittu 12 kuukauden Prepaid-sopimuksella.

1.1.2018 kello 15.00 käynnistetään nbl-m1-large palvelin Windows Server-käyttöjärjestelmällä ja 50 Gt SSD-levytilalla. Palvelimella ajetaan erilaisia rasitustestejä ja se tuhotaan kokonaisuudessaan tarpeettomana 4.1.2018 klo 12.00. Myös erikseen hankittus SSD-levytila poistetaan.

Prepaid tilaukset

Asiakkaalla on ympäristöön 3kpl nbl-hm1-medium Prepaid 1v tilauksia, sekä 1500 Gt SSD levyä

AIKA	YMPÄRISTÖ	PREPAID TILAU
1.1.2018 klo 15.00 asti	3 kpl nbl-hm1-large2000 Gt SSD	3KPL NBL-HM1
1.1.2018 klo 15.00 – 4.1.2018 klo 12.00	3kpl nbl-hm1-large1 kpl nbl-m1-large2050 Gt SSD	3KPL NBL-HM1
4.1.2018 klo 15.00 eteenpäin	3 kpl nbl-hm1-large2000 Gt SSD	3KPL NBL-HM1

Tammikuun veloitukset

Kuvaus
Prepaid nbl-hm1-large palvelimet (12kk)
Prepaid SSD (12kk)
Ondemand SSD ylimenevä 500 Gt((0,3€ /Gb*500Gb) / 43 200 min /kk=0,003472€ / min*31 pv. (Huom. 31 pv. kk)
Ondemand SSD – testijakso 50 Gt 69h ajanjaksolta
Ondemand nbl-m1-large 69h ajanjaksolta
Windows käyttöoikeus Ondemand palvelimeen
Tammikuun veloitukset yht.

HALLINTAPANEELI (CONTROL PANEL)

MISTÄ VOIN VAIHTAA SALASANANI?

Kirjaudu Cloud 9-hallintaan osoitteessa https://control.nebulacloud.fi. Paina yläpalkista kohta jossa lukee oma käyttäjätunnuksesi ja valitse avautuvasta pudotusvalikosta C**hange password**.

Syötä avautuvaan ikkunaan vanha salasana *(Current password)* sekä uusi salasana kahteen kertaan *(New password / Confirm new password)*. Klikkaa lopuksi **Change**.

SAANKO KOLLEGALLE OMAT HENKILÖKOHTAISET TUNNUKSET SAMAAN YMPÄRISTÖÖN?

Kyllä! Kirjaa työpyyntö MyNebula -portaalin kautta. Luvan antajan tulee olla projektin ylläpitäjä. Ilmoita mihin projektiin ja mille sähköpostiosoitteelle tulee liittää pääsy ympäristöön.

YRITYKSELLENI ON TÄRKEÄÄ SAADA EROTELTUA KUSTANNUKSET ASIAKKAITTAIN / KÄYTTÄJITTÄIN? MITEN TÄMÄ ONNISTUU?

Palvelua tilattaessa verkon kautta määritellään projektille nimi. Voit tilata palvelun useampaan kertaan asiakaskohtaisesti ja laittaa jokaiselle oman nimen. Näin laskulla voit tunnistaa omat asiakkaasi, sovelluksesi tai liiketoimintayksikkösi toisistaan. Voit liittää samat tai pyytää meitä liittämään pääsyn samoilla hallintatunnuksilla useisiin eri projekteihin.

PALVELIMET (INSTANCES)

MILLÄ TUNNUKSELLA KIRJAUDUN LINUX-PALVELIMELLE?

KÄYTTÄJÄTUNNUKSET

- Ubuntu palvelinten oletuskäyttäjätunnus on ”ubuntu”
- CentOS palvelinten oletuskäyttäjätunnus on ”centos”
- Root-tunnus on oletuksena disabloitu tietoturvasyistä. Pääkäyttäjäksi (root) pääset sudo -i komennolla.

AUTENTIKOINTI

- Toimittamissamme Imageissa autentikointi perustuu oletuksena sertifikaattiin, jonka käyttäjä ensin luo ”Access & Security” kohdassa ja palvelimen provisioinnin jälkeen autentikoi palvelimeen valitulla ”Key Pair” privaatti avaimella.
- Jos palvelimen luonnin yhteydessä ”Key Pair” on unohtunut määritellä, on helpointa tuhota palvelin ja tehdä uusi, sillä ilman avainparia et pääse kirjautumaan.

KÄYTTÄJÄTUNNUKSEN LUONTI “CUSTOMIZATION SCRIPT” AVULLA

- Palvelimen luonnin yhteydessä on mahdollista ajaa “user data / customization script” jolla voidaan luoda esimerkiksi käyttäjätunnukset palvelimelle.

MILLÄ TUNNUKSELLA KIRJAUDUN WINDOWS-PALVELIMELLE?

Oletuksena Windows-palvelimella on kaksi käyttäjätunnusta, Admin ja Administrator.

Administrator-käyttäjätunnuksen käyttöönotto

- Windows palvelimen salasana pitää käydä konsolin kautta muuttamassa ensimmäisen kirjautumisen yhteydessä. Salasana on tyhjä.
- Windows palvelimen konsolille pääset hallintapaneeli => Instances => ”Palvelimen nimi” => More => Console kautta.
- Ensimmäisen kirjautumisen jälkeen voit muodostaa etäyhteyden

Admin-käyttäjätunnuksen käyttöönotto

- Palvelimen Admin salasana voidaaan purkaa sertifikaattia vastaan joko konsolista tai komentoriviltä.

MITEN SAAN KÄYTETTYÄ USEAMPAA SERTIFIKAATTIA PALVELIMELLA?

Instanssiin voi luonnin yhteydessä määrittää avaimen mikä sinne järjestelmän puolesta asennetaan. Userdatan mukana avaimia voi viedä useamman esimerkiksi cloud-init:n kautta: https://cloudinit.readthedocs.org/en/latest/topics/examples.html#configu…

Voi laittaa tiedot suoraan instanssin luontivaiheessa “Post creation” välilehdelle.

Jälkikäteen järjestelmään tuodut avaimet eivät mene instansseille vaan se valitaan luontivaiheessa “Access & security”-välilehdeltä. Ainut tapa vaihtaa tuo avain on joko luoda instanssi uudelleen, jolloin datat, mitä käyttöjärjestelmälle varatuilla levyillä on tuhoutuu. Datat kannattaa tämän vuoksi pitää erillisellä Volume-levyllä.

MITEN SAAN ETÄYHTEYDEN PALVELIMEEN JONKA LOIN?

- Palvelimeen on lähtökohtaisesti estetty sisäänpäin tuleva liikenne ulkopuolisista aliverkoista. Käyttäjän tulee sallia ”Security Group” säännöstöllä että palvelimeen sallii SSH 22 tai RDP 3389 liikenteen palvelimelle.
- Windows-palvelimen salasana pitää käydä konsolin kautta asettamassa ensin ensimmäisen kirjautumisen yhteydessä

APUA, UNOHDIN SALASANAN PALVELIMEN!

- Jos et ole vielä vaihtanut Windows-palvelimen salasanaa voit noutaa sen tätä kautta. Konsolin kautta löytyy Compute => Instances => More => Retrieve Password -toiminto jolla voi sertifikaattia vastaan noutaa salasanan palvelimelle.

MITEN VOIN NOSTAA JA LASKEA PALVELIMENI RESURSSEJA?

- Palvelimen suorituskyky on määritelty ”flavor” kohtaisesti. Flavor on toimittajan valmiiksi määrittelemä konfiguraatio vCPU:ta, keskusmuistia sekä järjestelmälevyä. Voit muuttaa palvelimen konfiguraatiota suuremmaksi tai pienemmäksi muuttamalla palvelimen flavoria.
- Huomaathan että palvelimella ei saa olla järjestelmälevyllä enempää dataa kuin mikä on on valittu flavor koko, ja että palvelin käynnistyy uudelleen kun flavor konfiguraatio muutetaan

- Alaspäin skaalaus on tuettu ainoastaan, mikäli järjestelmälevy ei pienene, riippumatta data määrästä.

LEVYTILA

MITÄ LEVYÄ MINUN TULISI KÄYTTÄÄ TIEDOSTOJEN TALLENTAMISEEN?

On suositeltavaa että kaikki tärkeät tiedostot talletetaan ulkoiselle ”Volume” -tyyppiselle levylle. Näiden kokoa on mahdollista kasvattaa, näiden suorituskyky on tyypillisesti parempi ja Volume-tyyppisen levytilan voi siirtää palvelimelta toiselle.

MITEN SAAN PALVELIMESTANI VARMUUSKOPIOT?

Tähän on lukuisia eri vaihtoehtoja riippuen tarpeestasi

- Telia tarjoaa varmistuspalvelua – Ota yhteys myyntiin
- Voit kopioida datan eri saatavuusalueiden välillä ristiin
- Voit antaa palvelimet meidän hallintaamme, jolloin voimme hoitaa varmistukset puolestasi

Tutustu artikkeliin varmuuskopioinnista

VERKOT (NETWORK)

MITÄ IP-AVARUUKSIA VOIN KÄYTTÄÄ CLOUD 9-PALVELUN SISÄLLÄ?

Palvelussa on mahdollista rakentaa pilven sisäiset verkot käyttämällä privaattiosoitteita RFC1918 määritysten mukaisesti, eli seuraavat osoitteet ovat käytössä 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 192.168.0.0 – 192.168.255.255.

MITEN SALLIN LIIKENTEEN PALVELIMILLE?

Jokaiseen palvelimeen kohdistuu ”Security Group” sääntökanta. Security Group säännöt voivat esimerkiksi sallia HTTP liikenteen sisäänpäin. Oletusarvoisesti Security Group säännöt sallivat kaiken liikenteen ulospäin, sallivat sisäänpäin tulevan liikenteen samasta aliverkosta ja estävät eri aliverkosta sisäänpäin tulevan liikenteen, kuten Internetistä palvelimelle. Security Group sääntöjä voit muokata Instances => Access & Security kohdasta ja palvelinkohtaisesti määritellä mitkä Security Group säännöt kohdistuvat mihinkin palvelimiin.

ONKO PALVELUSSA ERILLISTÄ PALOMUURIA?

Palveluun kuuluu oletuksena ohjelmallinen palomuuri. Palomuuri kontrolloi liikennettä Internetin ja Asiakkaan verkkojen välillä. Palomuuria voi hallita Cloud 9 -hallinnasta Network => Firewalls kautta. Palomuuri tarkoittaa yhtä aktiivista sääntökantaa. Sääntökanta voi koostua useammasta säännöstä. Kun asiakas kytkee palomuurin päälle, se oletuksena estää kaiken muun liikenteen (sisään ja ulos) paitsi säännöillä sallitun liikenteen.

SAANKO LIITETTYÄ CLOUD 9:N OSAKSI YRITYSVERKKOANI?

Kyllä, ole yhteydessä myyntimme, niin autamme muodostamaan turvallisen yhteyden yritysverkkoosi. Tuettuja vaihtoehtoja on

- VPN yhteys ylläpitämästämme palomuuripalvelusta
- Symmetrinen 100Mb/s – 1000Mb/s IP-VPN valokuituyhteys

Voit myös itse tehdä yhteyden seuraavien ohjeiden mukaan

MITEN JULKISET IP:T TOIMIVAT?

Access & Security valikon kautta asiakas voi ottaa IP-osoitteet käyttöön saatavuusaluekohtaisesti. IP-osoitetta ei voi siirtää saatavuusalueelta toiselle. IP-osoite pysyy varattuna asiakkaalle kunnes asiakas vapauttaa sen. Asiakas voi hallintapaneelin kautta liittää IP-osoitteen haluamaansa palvelimeen saatavuusalueen sisällä.

ONKO PALVELIMEEN MAHDOLLISTA LIITTÄÄ USEITA VERKKOLIITÄNTÖJÄ ERI VERKOISTA?

Kyllä! Voit tehdä tämän palvelinta asentaessa graafiseen työkalun kautta. Jos palvelin on jo asennettu niin voit tehdä sen komentorivityökalulla seuraavalla komennolla.

nova interface-attach [–port-id <port_id>] [–net-id <net_id>] [–fixed-ip <fixed_ip>] <server>

API-RAJAPINTA

MITEN KÄYTTÖÖN?

Lue erillinen ohje komentorivityökalun asennuksesta.

LASKUTUS JA KAPASITEETTI

MISTÄ NÄEN KÄYTETYN KAPASITEETIN HINNOITTELUN?

VARATTU KAPASITEETTI – ASIAKKUUS PERUSTETTU ENNEN 11/2015

Palvelu on hinnoiteltu varatun kapasiteetin mukaan. Kuukausihinta muodostuu valitusta kapasiteettirajoista. Palvelinten, verkkojen tai levypintojen luominen tai poistaminen ei suoraan vaikuta laskutukseen. Kun valitset oikeasta yläkulmasta “Osta” painikkeen pääset yrityksen tiedot syötettyäsi sivulle, josta voit nähdä käyttöön varatun kapasiteetin sekä sen kuukausihinnan.

KÄYTÖN MUKAAN LASKUTETTU KAPASITEETTI

Kuukausihinta muodostuu tilatusta Prepaid-kapasiteetista, sekä tämän ylittävältä osalta On-Demand -veloituksesta minuutin tarkkuudella. Voit kirjautua MyNebula-portaaliin osoitteessa https://my.nebula.fi tarkastelemaan Prepaid-tilauksiasi.

MIKSI EN VOI ITSE VALITA MITEN PALJON PALVELIMELLANI MUISTIA TAI PROSESSOREITA?

Pilviympäristön toimivuus perustuu tehokkaaseen ja automatisoituun tapaan hyödyntää palvelimia. Kun ympäristöä rakennetaan, mitoitetaan ympäristö mahdollisimman tarkasti siellä ajettavien palvelimien mukaan. Pilven suunnittelussa optimoidaan mitkä virtuaalikoneet kannattaa ajaa milläkin palvelimella parhaan suorituskyvyn takaamiseksi. Näin vältetään tilanteita, joissa on esimerkiksi yliallokoitu kapasiteettia, niin että tämä heikentää asiakkaiden palvelunlaatua. Virtuaalipalvelimien täyttöä palvelimille voi ajatella legoina, jos väärän muotoisia palvelimia laitetaan liikaa voi jäädää joko tyhjää tilaa joka siirtyisi asiakkaalle kustannuksina vajaakäytöstä tai vastaava ylikäyttö johtaisi suorituskyky

ongelmiin. Samalla Telia mitoittaa myös riittävän määrän verkkokaistaa ja levyjärjestelmän suorituskykyä jokaiselle asiakkaalle. Tarjoamalla vakiodut rakennuspalikat varmistamme että asiakkaat saavat kustannustehokkaita ja suorituskykyisiä palveluita. Otamme kuitenkin mielellään asiakkailta toiveita vastaan millaisia palvelimia meidän olisi hyvä tulevaisuudessa tarjota!

MITEN VOIN LUODA TOISEN PROJEKTIN JA HALLINNOIDA SITÄ SAMALLA KÄYTTÄJÄTUNNUKSELLA?

Cloud 9-palvelussa jokaiseen projektiin liittyy uniikki, toimiva sähköpostiosoite, tämän lisäksi voi olla muita ylläpitotunnuksia. Tunnuksen pitää olla toimiva ensimmäisen salasanan toimitusta varten. Suosittelemme että toimit seuraavasti

1. Mene https://cloud9.nebula.fi sivulle
2. Valitse “Tilaa Nyt”
3. Syötä uniikki sähköpostiosoite, jota et aiemmin ole käyttänyt (ks. alla)
4. Syötä asiakasnumerosi
5. Valitse tarvittavat projektikohtaiset prepaid-resurssit
6. Palvelu on käytössä välittömästi
7. Avaa MyNebulasta palvelupyyntö, jossa kerrot mitkä muut sähköpostiosoitteet haluat liittää ylläpitäjiksi projektille

Useimmat sähköpostijärjestelmät tukevat virtuaalisten sähköpostiosoitteiden tekoa liittämällä + merkin ja sen jälkeen tunnisteen, esimerkiksi seuraavasti

matti.meikalainen@yritys.fi => **matti.meikalainen+betaprojekti@yritys.fi** – nämä ohjautuvat samaan postilaatikkoon.

Tulemme tuomaan käyttäjien hallinnointiominaisuuden, jolloin tämä kiertotarve poistuu.

MITEN HALLINNOIN PREPAID TILAUKSIA?

MITEN SAAN LISÄÄ KAPASITEETTIA?

TILAUKSET ENNEN 11/2015 – VARATUN KAPASITEETIN MUKAAN.

Valitsee hallinta konsolin oikeasta yläkulmasta “Osta”. Pääset yrityksen tiedot syötettyäsi sivulle, josta voit ostaa nähdä käyttöön varatun kapasiteetin sekä sen kuukausihinnan. Voit kasvattaa tällä sivulla sivulla yrityksesi kapasiteettia. Pienet tilaukset provisioidaan automaattisesti. Jos tilaat lisää niin että kokonaistilauksen arvo ylittää 100 euroa se käy vielä luottotarkistuksen läpi ja on yleensä käytössä noin tunnin-kahden kuluttua. Kapasiteetti tulee projektille, jonka hallintakonsoliin oli kytkeydytty.

TILAUKSET 11/2015 JÄLKEEN – KÄYTÖN MUKAAN LASKUTUS

Oletuksena uudella asiakkaalla resursseja on käytettävissä alla mainittu kapasiteeti. Rajoitukset kapasiteetissa ovat nostettavissa, ne suojaavat Asiakasta vahingossa tarkoituksettomalta liialliselta käytöltä.

- 64 vcpu

- 384 Gt RAM
- 1000 Gt SSD
- 2500 Gt SAS
- 5000 Gt ARK
- 20 Julkinen IP-osoite

Näiden resurssien käyttämisestä laskutetaan toteutuneen mukaan, minuutin tarkkuudella. Monella asiakkaalla tarve ylittää nämä rajat ja jos haluat samaan projektiin enemmän resursseja ole yhteydessä Asiakaspalveluumme. Levytilaa, CPU ja RAM määrää voidaan nostaa asiakkaan tarpeen mukaan. IP osoitteet ovat rajallinen resurssi ja yli 20 IP-osoitteen tarve on poikkeuksillinen, yleensä hyvällä suunnittelulla voidaan tarvetta vähentää oleellisesti.

TYYPILLISIÄ ONGELMIA

KOKEILIN LUODA PALVELIMEN, MUTTA SE EI JOSTAIN SYYSTÄ ILMESTY LISTAAN.

Tarkista seuraavat

- *Viekö haluttu palvelin enemmän kapasiteettia kuin mitä on kapasiteettia vapaana? Näet hallintakäyttöliittymästä vapaan kapasiteetin määrän.*
- *Oletko kokeilemassa luoda palvelinta pienemmälle levylle kuin mitä käyttöjärjestelmä vaatii? Windows-palvelin vaatii 32Gt levytilaa.*

KOKEILIN LIITTÄÄ JULKISEN IP-OSOITTEEN PALVELIMEEN, MUTTA TÄMÄ EI JOSTAIN SYYSTÄ ONNISTU?

Julkinen IP-osoite on aina saatavuusaluekohtainen. Onhan palvelin samalla saatavuusalueella kuin IP-osoite?

KOKEILIN LIITTÄÄ LEVYTILAA PALVELIMEEN, MUTTA TÄMÄ EI JOSTAIN SYYSTÄ ONNISTU?

Tarkista

- ”Volumes” Levytila on aina saatavuusaluekohtainen. Onhan palvelin samalla saatavuusalueella kuin määritelty levytila?
- Näkyykö palvelimella ulkoisia asemia, jotka ei ole liitetty osaksi tiedostojärjestelmää?

Alaotsikko: INCLOUD: PARHAITA KÄYTÄNTÖJÄ

ARKKITEHTUURI

1. **Automatisoi infrastruktuurin pystytys** Hyödynnä automaatiotyökaluja, kuten Ansible ja Heat, joilla voit automatisoida ympäristön pystytyksen.
2. **Hajauta kahdelle saatavuusalueelle** Cloud 9 huoltokatkot suoritetaan eri aikaa eri saatavuusalueilla. Tällöin varmistat, palvelusi toimivuuden myös huoltokatkojen aikana.

3. **Tallenna data ulkoisille levyille** Palvelimen käyttöjärjestelmälevyä ei voi kasvattaa, eikä suorituskykyä säätää. Suosittelemme käyttämään ulkoisia levyalueita, jotka tarjoavat paremman suorituskyvyn ja skaalautuvuuden. Lisäksi ne voi siirtää palvelimelta toiselle joustavasti.
4. **Käytä versionhallintaa** Kun automatisoit infrastruktruurin, voit tallentaa voimassa olevan version versionhallintaan. Näin sinulla on aina dokumentaatio olemassa.

WINDOWS

1. **Vältä Hot-Plug liitäntöjä verkoissa** Jos verkkokortti liitetään palvelimen ollessa käynnissä, on riski että uudelleenkäynnistyksen yhteydessä verkkokortit menettävät konfiguraationsa.
2. **Vältä Hot-Plug liitäntöjä uusisa levyalueissa** Jos levytila liitetään palvelimen ollessa käynnissä, on riski että uudelleenkäynnistyksen yhteydessä levyalueet jäävät “offline” tilaan.
3. **Suorita laitteistomuutoksen jälkeen palvelimen alasajo sammuttamalla** Laitteiden PCI-osoitteet saattavat muuttua ensimmäisen sammutus-käynnistys sekvenssin yhteydessä.
4. **Huomioi UTC-aikavyöhyke** Pilviympäristöissä host palvelimet käyttävät aina UTC-aikaa. Huomioi tämä palvelimen asetuksissa. Jos muuta määritellä asetuksiin tulee palvelin palaamaan UTC aikaan viimeistään, kun host palvelin päivitetään / käynnistetään uudelleen.
5. **Älä nimeä uudestaan** Jos palvelimen nimen muuttaa, voi pilven automatiikka joissain tilanteissa pakottaa palvelimelle alkuperäisin nimen. Tämä voi tapahtua esimerkiksi palvelimen kokoa muutettaessa.

Alaotsikko: INCLOUD: NELB-KUORMANTASAUKSEN PALVELUKUVAUS

NELB-KUORMANTASAUS

NELB eli Nebula Elastic Load Balancer on INcloud 9 -palveluun saatavilla oleva lisäpalvelu. Palvelun avulla voidaan hajauttaa sisääntulevaa internet-liikennettä usealle eri palvelimelle ja/tai hyödyntää kumpaakin saatavuusaluetta. Saatavuusalueisiin hajauttamalla varmistetaan palveluiden katkoton toiminta esim. huoltotöiden yhteydessä. Huoltotyöt ajoitetaan aina vain yhdelle saatavuusalueelle kerrallaan.

Kuormantasauksen lisäksi palvelulla voidaan myös suorittaa verkkoliikennettä salaavien SSL-sertifikaattien purkamista. SSL on kasvattanut merkitystä huomattavasti sivustolla vierailevien kävijöiden silmissä. Kävijät haluavat varmistaa, että heidän vierailunsa on turvallinen ja mahdolliset sivuston kautta tehdyt yhteydenotot tai verkkokauppatilauksissa kulkevat tiedot ovat salassa.

Sertifikaatin hyödyt eivät rajoitu ainoastaan dataliikenteen salaukseen. Google on jo pitkään hakutuloksissaan nostanut ylemmäksi sivustoja, joissa hyödynnetään SSL-sertifikaatteja. Myös selainvalmistajat varoittavat salaamattomasta sivustosta jatkuvasti aggressiivesimmilla tavoilla.

Palvelun käyttöönotto on nopeaa ja helppoa. Riittää että NELB-palvelu luodaan palvelimien hallintaan tarkoitetussa palvelussa https://control.nebulacloud.fi.

Löydät palvelun ylälaidan valikosta Network > Nebula Elastic LoadBalancer. Tämän jälkeen palvelu veloitetaan normaalin laskutuksen yhteydessä On-Demand-veloituksena.

NELB-palvelun konfigurointiin liittyvät ohjeet löytyvät osoitteesta: https://tuki.inmicsnebula.fi/nelb-kuormantasaus/

Myyntimme auttaa sinua, mikäli palvelu herätti kysymyksiä.
Yhteystietomme löytyvät osoitteesta: https://www.inmicsnebula.fi/fi/yhteystiedot

Miksi palvelu tulisi hajauttaa?

Nykyisin internetissä toimiviin palveluihin kohdistuu painetta jatkuvasta toimivuudesta. Usein palvelut ovat yksittäisten palvelimien varaan rakennettuja eli sivusto, tietokanta ja ehkä myös sähköpostit ovat kaikki samalla yksittäisiellä palvelimella. Tämän vikaantuminen aiheuttaa täten katkoksten koko yrityksen toimintaan.

Hajauttamalla palveluita eri palvelimille saatavuusalueen sisällä ja kahdentamalla järjestelmä INcloud 9 -palvelun mahdollistamaan kahteen saatavuusalueeseen, minimoidaan riski siihen, että koko yrityksen kriittiset toiminnot ovat käyttämättömissä.

Yhden saatavuusalueen sisällä voidaan tehdä myös hajauttamista siten, että luodaan erikseen palvelimet hoitamaan tietokantakyselyitä ja omat palvelimet sivustokyselyitä. Tällöin esim. sivustoa hoitavia palvelimia voi olla saman saatavuusalueen sisällä useita ja NELB tasaa näihin liikennettä, jotta yksittäisen palvelimen kuormitus ei aiheuta hidastumista sivustolatauksessa.

Voitteko auttaa minua suunnittelemaan ja rakentamaan palveluiden hajauttamisen?

Tämä onnistuu. Asiantuntijoillamme on vuosien kokemus erityyppisten ja kokoisten kriittisten järjestelmien suunnittelusta ja toteutuksesta.

Määrittelemme tarvittavat säännöstöt sovelluksellesi, asennamme kuormantasajaat ympäristöösi ja voimme ottaa vastuun myös näiden jatkuvasta toimivuudesta. Palvelu on erikseen veloitettavaa asiantuntijatyötä.

Alaotsikko: INCLOUD: AVAINTEN HALLINTA

Tämä ohje on tarkoitettu käyttäjille, jotka asentavat unix-pohjaisia instansseja Pilveen ja on epäselvää miten käyttäjähallinta pitää tehdä.

Tietoturva

Huomaathan että SSH-pääsy palvelimelle maailmalta (0.0.0.0/0) mahdollistaa hakkereiden bruteforce-hyökkäykset varsinkin jos salasana-kirjautuminen on mahdollistettu. Suosittelemme palomuuraamaan palvelimen SSH-pääsyn mahdollisimman tiukasti.

Avaimia ei voi Pilvestä instanssin luonnin jälkeen myöhemmin enää vaihtaa tai lisätä. Valittu avain on ainoa tapa päästä palvelimeen käsiksi heti asennuksen jälkeen.

Pilvessä tarjolla olevissa Linux-imageissa on oletuksena salasana-tunnistautuminen SSH:n yli estetty, joten oletuskäyttäjälle (centos, debian, ec2-user, ubuntu) asetettu salasana ei SSH:n yli toimi. Pilven hallintapaneelissa konsolin kautta instanssiin kuitenkin pääsee sisään salasanalla heti kun käyttäjä on asettanut salasanan tunnukselle.

Luodessasi instanssia valitse Key pair (avainpari) käyttöön, ja asennuksen jälkeen kirjaudu palvelimelle sisään. Tästä eteenpäin käyttäjähallinta pitää tehdä käsin, Pilven hallinta ei voi enää osallistua avainten lisäämiseen tai poistamiseen. Käyttäjien ja avainten hallinta on siis tehtävä niinkuin instanssi olisi normaali palvelin.

Käytettävissä on tässä ohjeessa viisi mallia:

1.Yksi käyttäjä, Jaettu avain (ei suositeltu)

Jokaiselle instanssin käyttäjälle jaetaan sama private-avain, kaikki kirjautuvat samalla avaimella oletuskäyttäjänä sisään. Emme suosittele tätä mallia tietoturvasyistä, avain voi vahingossa levitä vääriin käsiin monesta eri lähteestä.

2.Yksi hyppypalvelin, useita käyttäjiä

Voitte tallentaa private-avaimen omalle hyppypalvelimelle (bastion) ja antaa käyttäjille oikeudet käyttää avainta esim sudo-mekanismin läpi

sudo –u pilviuser ssh centos@x.x.x.x

Näin jos tulee uusia palvelimia tai avaimia vaihdetaan, vaihtaminen hyppypalvelimelta riittää. Avainta/avaimia ei koskaan tarvitse jakaa käyttäjille.

3.Yksi käyttäjä, monta avainta

Käyttäjät lähettävät ylläpitäjälle oman avainparinsa julkisen puolen (public). Ylläpitäjä käy lisäämässä palvelimella oletuskäyttäjän authorized_keys tiedostoon kaikkien public-avaimet.

4. Monta käyttäjää, monta avainta (suositeltu)

Kirjaudu instanssille asennuksen jälkeen ja luo jokaiselle käyttäjälle henkilökohtainen tunnus, ja tallenna käyttäjien julkiset avaimet kunkin authorized_keys tiedostoon.

ssh centos@x.x.x.x sudo -i useradd petri useradd mikko useradd maija echo "ssh-rsa xxzzyy..." > ~petri/.ssh/authorized_keys echo "ssh-rsa yyzzxx..." > ~mikko/.ssh/authorized_keys echo "ssh-rsa zzyyxx..." > ~maija/.ssh/authorized_keys for x in `ls /home`; do chown -R $x /home/$x; done

5. Monta käyttäjää, salasanatunnistautuminen (ei suositeltu)

Kirjaudu instanssille asennuksen jälkeen ja luo jokaiselle käyttäjälle henkilökohtainen tunnus, aseta käyttäjille salasanat. Muokkaa /etc/ssh/sshd_config tiedostoa ja salli salasanatunnistautuminen. Ilmoita käyttäjille henkilökohtaiset käyttäjätunnukset ja salasanat.

Tarkista /etc/cloud/cloud.cfg tiedostosta asetukset ettei Pilven cloud-init nollaa sshd_config –asetusta uudelleenkäynnistyksessä.

Emme suosittele salasanakirjautumisen mahdollistamista lainkaan.

Myös oletuskäyttäjälle voi asettaa salasanan mutta emme tietoturvasyistä listaa sitä vaihtoehdoksi, emme missään nimessä suosittele sitä. Riippuen cloud-init asetuksista, oletuskäyttäjän salasanakin voi vaihtua uudelleenkäynnistyksessä.

Alaotsikko: INCLOUD: VAHVA TUNNISTAUTUMINEN

Voit lisätä tietoturvaa INcloud 9-palvelussa ottamalla käyttöön vahvan tunnistautumisen. Vahva tunnistauminen perustuu TOTP teknologiaan ja helpoiten käytät sitä älypuhelimellasi.

Ominaisuuden avulla kirjautumiseen tarvitaan sovelluksen antama vaihtuva koodi, eikä pelkkä käyttäjätunnus salasana yhdistelmä riitä kirjautumiseen.

Alaotsikko: INCLOUD: OMINAISUUDET

COMPUTE (NOVA)

Compute-moduuli on alustan ydin, jolla hallitaan palvelimia (instances) ja verkkoja.

Palvelimet sijaitsevat fyysisesti jommalla kummalla kahdesta eri saatavuusalueesta **(Availability zone)**. Kukin palvelin perustuu mallipohjaan **(Flavor)**, jotka ovat ennalta määritettyjä palvelinkonfiguraatioita. Palvelimen voi skaalata joko alas- tai ylöspäin annettujen konfiguraatiopohjien puitteissa.

Ilmaisen kokeilujakson **(FREE-TIER)** resurssit on suunniteltu kokeilukäyttöön. Näiden instanssien suorituskyky on tarkoitettu testaamiseen, eikä niiden suorituskyky kuvaa Pilven todellista suorituskykyä. Kokeilujaksopalvelinten verkkoliikenteen määrä ja levy-IO on rajoitettu kapasiteetin turvaamiseksi.

NIMI	KOKOONPANO
NBL-FREE-TIER	1 CPU 768MB, 32 Gt järjestelmälevyä
NBL-N1-TINY	1 CPU, 1Gt, 32Gt järjestelmälevyä
NBL-N1-SMALL	1 CPU, 2Gt, 150Gt järjestelmälevyä
NBL-N1-MEDIUM	2 CPU, 4Gt, 150Gt järjestelmälevyä
NBL-N1-LARGE	4 CPU, 8Gt, 150Gt järjestelmälevyä

NBL-N1-XLARGE	8 CPU, 16Gt, 150Gt järjestelmälevyä
NBL-N1-2XLARGE	16 CPU, 32Gt, 150Gt järjestelmälevyä
NBL-M1-SMALL	1 CPU, 4Gt, 150Gt järjestelmälevyä
NBL-M1-MEDIUM	2 CPU, 8Gt, 150Gt järjestelmälevyä
NBL-M1-LARGE	4 CPU, 16Gt, 150Gt järjestelmälevyä
NBL-M1-XLARGE	8 CPU, 32Gt, 150Gt järjestelmälevyä
NBL-M1-2XLARGE	16 CPU, 64Gt, 300Gt järjestelmälevyä
NBL-HM1-LARGE	2 CPU, 16Gt, 300Gt järjestelmälevyä
NBL-HM1-XLARGE	4 CPU, 32Gt, 300Gt järjestelmälevyä
NBL-HM1-2XLARGE	8 CPU, 64Gt, 300Gt järjestelmälevyä
NBL-HM1-4XLARGE	16 CPU, 128Gt, 300Gt järjestelmälevyä

Oletuksena palvelimen käyttöjärjestelmä asennetaan paikalliselle levylle, joka ei ole pysyvää levytilaa. Tämä tarkoittaa sitä, että palvelimen tiedot säilyvät esim. uudelleen käynnistyksen yhteydessä, mutta palvelimen poistamisen yhteydessä kaikki sinne tallennetut tiedot häviävät. Pysyvämpään tarpeeseen kannattaa pitää tiedostot erillisellä massamuistilla **(Volume)**, joka voidaan tarvittaessa liittää toiseen palvelimeen.

IMAGET (LEVYKUVAT)

Palvelussa on tarjolla useita valmiita levykuvia eri käyttöjärjestelmillä varustettuna. Voit valita halutun levykuvan palvelimen luontivaiheessa.

KÄYTTÖJÄRJESTELMÄ	VARAA TILAA JÄRJE
CentOS 7 (x86_64)	326.7 MB
CentOS 6 (x86_64)	1.1 GB

Debian 9 (x86_64)	574.85 MB
Debian 8 (x86_64)	604.01 MB
Debian 7 (x86_64)	997.3 MB
Ubuntu 16.04 (x86_64)	276.31 MB
Ubuntu 14.04 (x86_64)	250.63 MB
Windows Server 2016 (Datacenter 64-bit)	14.91 GB
Windows Server 2012 (Datacenter 64-bit)	23.43 GB
Windows Server 2008 (R2 Datacenter 64-bit)	16.28 GB

Palveluun on myös mahdollisuus tuoda omia levykuvia.

LEVYTILA (CINDER)

Pysyvämpää levytilan tarvetta varten voidaan tiedot tallentaa levytilaan **(Volumes)**. Levytila on palvelimesta riippumaton levyosio, toisin kuin palvelimen oma paikallinen levytila.

Levytila voidaan luoda käyttäen hallintapaneelia tai API-rajapintaa. Levytilan kokoa rajoittaa ainoastaan palveluun hankittu kokonaiskapasiteetti **(Quota)** ja aiemmin käytetty levyn määrä. Kun levy luodaan ensimmäisen kerran, se on tyhjä levy ilman osioita tai tiedostojärjestelmää. Levy pitää ensin liittää palvelimeen **(Attach)** jotta se voidaan alustaa käyttöön, ja vielä sen jälkeen liittää käyttöjärjestelmään **(Mount)** jotta sille voi tallentaa tiedostoja.

Levyn voi liittää vain yhteen palvelimeen kerrallaan. Levy voidaan kuitenkin irrottaa palvelimelta ja liittää toiseen palvelimeen.

Levytila on käytettävissä vain yhden saatavuusalueen sisällä.

NIMI	**PAIKALLINEN LEVY**
Käyttötarkoitus	Käyttöjärjestelmä
Käyttö	Tiedostojärjestelmä
Saatavuus	Palvelimen sisällä

Säilyy kunnes	Palvelin poistetaan
Koko	Palvelinkonfiguraation (flavor) määrittämä

CLOUD 9 SISÄLTÄÄ KOLMEA ERITYYPPISTÄ LEVYPINTAA:

LEVYN TYYPPI	FYYSINEN LEVY	KÄYTTÖTARKOITUS	SUORITUSKYKY
LTK-SSD	SSD	Tietokanta, sovellusvälimuisti	50000 IOPS luku
LTK-SAS	NL-SAS	Sovellukset, staattinen data	3000 IOPS luku /
LTK-ARK	SATA	Arkisto,staattinen data, varmuuskopiot	1500 IOPS luku /

TILANNEKUVAT (SNAPSHOT)

Levyn tilannekuva on kopio levyn tilanteesta annettuna aikana. Yleisesti tilannekuva saatetaan ottaa jotta voidaan luoda uusi samanlainen levytila.

Levykuvaan tallentuu tiedostojärjestelmän nykyinen tila, mutta ei muistin tila.

Huomaathan, että levykuvaa ei kannata käyttää varmuuskopiona, sillä se tallentuu samalle fyysiselle laitteelle kuin missä lähdelevy on. Siitä voi olla apua palautustilanteessa esim. inhimillisen virheen jälkeen, mutta ei fyysisen laitevian kohdatessa.

VERKKOJEN HALLINTA (NEUTRON)

Neutron on alustan verkkojenhallintamoduuli, **“networking as a service”**. Sillä voidaan luoda virtualisoitu verkkoinfrastruktuuri, sisältäen verkkoja, reitittimiä ja palomuureja. Palvelimet ovat yhteydessä verkkoihin, jotka käyttävät sisäverkon IP-osoitteita, jotka voit itse määrittää. Reitittimiä käytetään tilanteessa jossa palvelinten on saatava yhteys ulkomaailmaan julkiseen Internetiin. Järjestelmän ulkopuolelta palvelimille pääsee käyttäen julkisia IP-osoitteita **(floating IP addresses)**. Liikenteen rajoittamiseksi verkon tasolla voidaan käyttää palomuuria.

Telia Pilven sisällä palvelinten tulee viitata toisiinsa vain sisäisillä ip-osoitteilla. Näin varmistetaan, että palvelun sisäinen liikenne pysyy virtuaalisen verkon sisällä.

HALLINTAPANEELI (HORIZON)

Horizon on selainpohjainen hallintapaneeli, jota voidaan käyttää palvelun hallintaan. Se sisältää helppokäyttöisen käyttöliittymän palvelun eri moduulien hallintaan ja sisältää seuraavat ominaisuudet:

- Palvelinten luominen ja hallinta
- SSH-avainten luominen ja hallinta
- Levypinnan hallinta

- Levykuvien hallinta
- Turvamääritysten hallinta
- Verkkojen, reitittimien ja palomuurien hallinta

SAATAVUUSALUEET (AVAILABILITY ZONES)

Cloud 9 sijaitsee useissa fyysisissä sijainneissa, jotka on eristetty toisistaan. Palvelussa näitä kutsutaan saatavuusalueiksi **(Availability Zones)**. Jokainen saatavuusalue on sijoitettu erilliseen Telian palvelinkeskukseen, joilla on toisistaan riippumattomat resurssit ja komponentit. Palvelinkeskuksilla on omat virtalähteet, UPS-järjestelmät ja automaattiset varavirtakoneet.

SAATAVUUSALUE	**SIJAINTI**
Helsinki-1	Helsinki, Lauttasaari
Helsinki-2	Helsinki, Pitäjänmäki

Palvelinkeskuksen vikaantuminen on harvinaista mutta mahdollista. Jos käytössä olevat palvelimet ja sovellukset on rakennettu vain yhden, vikaantuneen saatavuusalueen sisälle, mitkään palvelimista eivät ole saatavilla. Siksi on tärkeää rakentaa palvelimet ja ympäristön arkkitehtuuri hajautetusti molempiin saatavuusalueisiin. Myös yksittäisten komponenttien kuten verkkolaitteiden tai isäntäpalvelimien vikatilanteet ovat mahdollisia. Mahdollisten laitevikojen vaikutuksilta voi välttyä hajauttamalla palvelut useampaan saatavuusalueeseen.

Kaikki verkkoliikenne saatavuusalueiden välillä kulkee Telian omaa huippunopeaa runkoverkkoa pitkin.

MODUULI	**RESURSSI**	**SI**
Compute	Palvelimet	Yk
Volumes	LTK-SSD, SAS, ARK	Yk
Network	Julkiset IP-osoitteet	Yk
Palvelun sisäiset verkot	Useita saatavuusalueita	

Koska tiedostoja ei replikoida saatavuusalueiden välillä, on tärkeää rakentaa ympäristö eri saatavuusalueille ja tehdä replikointi palvelimilla, esim. tietokantareplikointi tai hajautettu tiedostojärjestelmä.

Kaikki palvelun hallintaan liittyvät elementit, mm. avainten hallinta, rajapinnat sekä käyttöliittymä sijaitsevat aina useammalla saatavuusalueella.

Kaikki Cloud 9 palveluun tallennettu sisältö on sijoitettuna ainoastaan Telian omiin palvelinkeskuksiin.

TURVAMÄÄRITYKSET (SECURITY GROUPS)

Security group, turvamääritykset, tarkoittaa virtuaalista palomuuria joka kontrolloi verkkoliikennettä sekä lähtevää että saapuvaa liikennettä palvelimella. Saapuvasta liikenteestä käytetään termiä *ingress* ja lähtevää liikennettä kutsutaan termillä *egress*. Oletuksena palvelussa on turvamääritys joka estää kaiken sisäänpäin tulevan liikenteen. Turvamäärityksiä voi luoda useampia ja jokaiseen määritykseen voi luoda sääntöjä, joilla voi hallita yksittäisiin palvelimiin kohdistuvaa liikennettä.

HUOM! Turvamäärityssääntöjen määrä on rajoitettu!

Alaotsikko: INCLOUD: PIKAOPAS

1. YHTEENVETO

Tämä dokumentti on INcloud 9 -palvelun pikaopas ja sen tarkoituksena on auttaa asiakasta luomaan ensimmäinen palvelin sekä ottamaan tähän etäyhteys.

2. YLEISET EHDOT

Tilausvaiheessa hyväksyttävät, Palvelua koskevat yleiset sopimusehdot löytyvät Telia Finland Oyj:n verkkosivuilta. Laaja kuvaus palvelun sisällöstä sekä rajauksista löytyy Palvelun palvelukuvauksesta.

3. PALVELUN KÄYTÖN ALOITTAMINEN

3.1. ILMAINEN KOKEILUJAKSO

Palvelun käyttö voidaan aloittaa luomalla tunnukset MyNebula-palveluun. Asiakkaalle toimitetaan tunnukset palveluun, sekä testikäyttöön soveltuva määrä kapasiteettia. Ilmaisen kokeilujakson erottaa vain rajoitettu kapasiteetin määrä. Mikäli Asiakas haluaa lisää kapasiteettia, on palvelu päivitettävissä maksulliseen versioon.

3.2. MISTÄ VOIN KIRJAUTUA PALVELUUN?

Palvelun hallintakäyttöliittymään kirjaudutaan verkkoselaimen kautta osoitteessa: https://control.nebulacloud.fi. Syötä kirjautumissivulle tilausvahvistuksessa saamasi käyttäjätunnus ja salasana.

4. KÄYTÖN ALOITTAMINEN

4.1. SSH-AVAIMEN LUOMINEN

Palvelun käyttö aloitetaan SSH-avainparin luomisella. Tallenna avainparin yksityinen osa (Private Key) eli .pem -tiedosto sellaiseen paikkaan, mihin vain avainta tarvitsevilla henkilöillä on pääsy, ja josta avaimen saa helposti käyttöön. Yksityisen avaimen haltijalla on pääsy mille tahansa palvelimelle, johon avainpari on liitetty. Tiedostosta kannattaa heti ottaa varmuuskopio!

SSH-avainparin avulla parannetaan palvelun tietoturvaa, sillä ainoastaan yksityisen avainparin haltijalla on mahdollisuus hallita palvelimia. **Huomaathan, että SSH-yhteys palvelimelle ei onnistu, ellei avainparia ole luotu ennen palvelimen luomista ja avainparia liitetä palvelimeen palvelimen luomisen yhteydessä. Avainparia ei voida liittää palvelimeen jälkikäteen!**

Aloittaaksesi SSH-avaimen luonnin, avaa pudotusvalikko **”Compute”** ja valitse pudostusvalikosta valinta **”Access & Security”**. Pudotusvalikko löytyy hallintakäyttöliittymän vasemmasta yläkulmasta.

Kun sinulle aukeaa **Access & Security** –sivu, siirry välilehdelle **”Key Pairs”** ja klikkaa **”+ Create Key Pair”**.

Syötä seuraavaksi SSH-avaimen nimi ja klikkaa **”Create Key Pair”**.

Omaa yksityistä SSH-avainta ei tallenneta Telia Pilvi –palveluun. SSH-avainta ei saa ladattua ja tallennettua enää myöhemmin uudelleen. (= Mikäli avain kadotetaan, menetetään samalla mahdollisuus hallita palvelinta/palvelimia, johon avain on liitetty).

4.2. VERKON LUOMINEN

Verkot on valmiiksi luotu molemmille saatavuusalueille ja vastaavat tyypilliseen tarpeeseen. **Siirry kappaleeseen 4.4.**

4.3. REITITTIMEN LUOMINEN

Reittimet on valmiiksi luotu molemmille saatavuusalueille ja vastaavat tyypilliseen tarpeeseen.. S**iirry kappaleeseen 4.4.**

4.4. SECURITY GROUP:N LUOMINEN

Ennen palvelinten luomista palveluun tulee määrittää Security Group:it. Security Groupin tarkoitus on helpottaa palvelimille tapahtuvaa liikenteen hallintaa sekä parantaa palvelun tietoturvaa. Seuraavissa ohjeissa luodaan esimerkkinä Security Group, jonka avulla sallitaan palvelimille SSH-yhteydenotot kaikkialta.

Aloita Security Group:in luominen siirtymällä pudotusvalikkoon **”Compute”** ja valitse pudotusvalikosta valinta **”Access & Security”**.

Kun sinulle aukeaa Access & Security –sivu, siirry välilehdelle **”Security Groups”**. Sivulla tulisi näkyä valmiina Security Group (default), joka sallii oletuksena liikenteen kyseiseen ryhmään kuuluvien instanssien välillä. Voit luoda lisää Security Groupeja halutun määrän tarpeesi mukaisesti.

Aloita Security Group:in luominen klikkaamalla **”+ Create Security Group”**.

Syötä tämän jälkeen ruudulle aukeavaan ikkunaan Security Group:in nimi ja kuvaus. Klikkaa tämän jälkeen **”Create Security Group”**.

Aloita Security Group:in sääntöjen lisääminen klikkaamalla juuri luodun Security Groupin perässä olevaa painiketta **”Manage Rules”**.

Lisää sääntöjä klikkaamalla auenneelta sivulta **”+ Add Rule”**.

Rule – Kenttään voi valita useita valmiita sääntöjä tai luoda kustomoidun säännön (custom rule). Tämän kentän valita rippuu siitä, mitä kenttiä sinun tulee täyttää seuraavaksi. Voit testimielessä lisätä säännön SSH-yhteyden sallimisesta (yhteys palvelimen porttiin 22). Valitse silloin tähän kenttään SSH.
Direction – *Ingress* = Saapuva, *Egress* = Lähtevä.
Port – Sääntöä koskeva portti.
Remote – Kenttään määritetään, mistä Rule-kentän mukaisen yhteyden ottaminen sallitaan.
Valitse **“CIDR”**, jolloin saat erikseen määrittää verkon, josta SSH-yhteys sallitaan.
CIDR – Määrittele tähän kenttään verkko, josta Rule-kentässä määritetyn yhteyden ottaminen sallitaan. Testimielessä voit jättää tähän oletusarvon 0.0.0.0/0, jolloin yhteydenotot SSH-protokollalla sallitaan kaikkialta (Yhteyden muodostamiseen tarvitaan toki edelleen vain sinulla hallussa oleva SSH-avain).

Klikkaa tämän jälkeen **”Add”**.

4.5. PALVELIMEN LUOMINEN

Aloita palvelimen luominen siirtymällä pudotusvalikkoon **”Compute”** ja valitse pudotusvalikosta valinta **”Instances”**.

Aloita palvelimen luominen klikkaamalla **”+ Launch Instance”**.

Ruudulle avautuu tämän jälkeen uusi ikkuna palvelimen luomista varten. Syötä kenttiin:

Availability Zone – Saatavuusalue (palvelimen lokaatio). **(Huom! Kun lisäät hetken kuluttua palvelinta verkkoon, varmista, että verkko on samalla saatavuusalueella.)**
Instance Name – Palvelimen nimi
Flavor – ”palvelupaketti”. Määrittää palvelimen kapasiteetin ja käytössä olevat resurssit, jotka kuvataan oikean laidan Flavor Details –laatikossa.
Instance Count – Luotavien palvelimien määrä
Instance Boot Source – Uuden palvelimen asennusmedia. Valitse esimerkiksi **“Boot from image”**, jolloin saat valita seuraavasta kentästä Imagen (levykuvan), josta palvelin luodaan.
Image name – Valitse image haluamallasi käyttöjärjestelmällä. Imagen nimen perässä lukee sen viemä levytila. (Huom! Varmista, että palvelimesi levytila riittää tähän kohdasta **”Flavor Details”** – **”Root Disk”**)

Lisää tämän jälkeen SSH-avain välilehdellä **”Access & Security”**. (Huom! Mikäli unohdat tämän vaiheen, palvelimesi ei salli mitään kirjautumisia. Mikäli unohdat tämän vaiheen, palvelin on luotava uudelleen, sillä SSH-avainta ei voi lisätä enää palvelimen lisäämisen jälkeen). Samalla välilehdellä voit myös lisätä palvelimelle Security Group:it.

Lisää tämän jälkeen palvelin verkkoon **”Networking”**-välilehdellä klikkaamalla verkon nimen perässä olevaa **”+”** -merkkiä. **(Huom! Liitä palvelin saman saatavuusalueen (Availability Zone) verkkoon, johon olet lisäämässä palvelintasi).**

Kun olet valmis, klikkaa **”Launch”**.

4.6. SECURITY GROUP:IN LIITTÄMINEN PALVELIMEEN

Mikäli suoritit Security Group:ien lisäämisen ja palvelimen luonnin yhteydessä, **voit siirtyä kappaleeseen 4.7.**

Siirry pudotusvalikkoon **”Compute”** ja valitse pudotusvalikosta valinta **”Instances”**. Etsi aukeavasta listauksesta palvelin, johon haluat liittää Security Group:in klikkaamalla palvelimen rivin perästä **”More”** ja valitse pudotusvalikosta **”Edit Security Group”**.

Liitä aiemmin luotu Security Group palvelimeen klikkaamalla vasemman reunan Security Group:in nimen perässä olevaa **”+”** –painiketta. Klikkaa tämän jälkeen **”Save”**. Voit poistaa palvelimen jostakin Security Group:ista klikkaamalla oikean puolen Security Group:in nimen perästä **”-”** –painiketta.

4.7. JULKISEN IP-OSOITTEEN LISÄÄMINEN PALVELIMELLE

Siirry pudotusvalikkoon **”Compute”** ja valitse pudotusvalikosta valinta **”Access & Security”**.

Siirry välilehdelle **”Floating IPs”**. Klikkaa **”Allocate IP To Project”**.

Ruudulle aukeaa ikkuna, jossa pääset valitsemaan saatavuusalueen, josta IP-osoite allokoidaan. **Huom! Varmista, että Pool-pudotusvalikkoon on valittu sama saatavuusalue (availability zone) kuin, jonka valitsit palvelimellesi ja verkollesi. Klikkaa tämän jälkeen ”Allocate IP”.**

Uusi IP-osoite ilmestyy hetken kuluttua ruudulla näkyvään listaukseen. Vapaan IP-osoitteen tunnistaa siitä, että sillä on **”Instance”** sarakkeessa pelkkä viiva **(”-”)** eli sitä ei ole lisätty millekään palvelimelle. Klikkaa halutun rivin perästä **”Associate”** –painiketta.

Ruudulle avautuu tämän jälkeen ikkuna, jossa on kaksi pudotusvalikkoa. Valitse ylempään pudotusvalikkoon haluttu IP-osoite ja alempaan haluttu palvelin. Klikkaa tämän jälkeen **”Associate”**.

5. YHTEYDEN MUODOSTAMINEN (LINUX PALVELIMEEN)

5.1. SSH-AVAIMEN TIEDOSTOTYYPIN MUUTTAMINEN

Otamme esimerkkitapauksessa yhteyden palvelimeen käyttämällä tunnettua SSH-yhteysohjelmaa nimeltä **Putty**. Koska Telia Pilvi tallentaa SSH-avaimen käyttämällä tiedostotyyppiä **.pem**, jota Putty ei tue, tiedostotyyppiä on muutettava.

Lataa Puttygen klikkaamalla seuraavaa linkkiä: PuTTY-lataussivusto Etsi listasta PuTTYgen ja klikkaa sen jälkeen olevaa linkkiä **”puttygen.exe”**.

Kun olet ladannut ja avannut **PuTTYgen**-sovelluksen klikkaa sovelluksesta painiketta **”Load”** ja valitse Telia Pilvestä laatamasi SSH-avain. Kun etsit tiedostoa, varmista, että sinulla on **aktivoituna kaikkien sovellustyyppien etsintä.**

Kirjoita seuraavaksi sovellukseen haluamasi salasana avaimen käyttöä varten (huom! tarvitset sitä myöhemmin) ja klikkaa **”Save private key”**. Salausavain tallennetaan nyt **.ppk**-tiedostotyyppiä käyttäen. Valitse tallennuskansio ja muista ottaa talteen myös valitsemasi salasana.

5.2. SSH-YHTEYDEN MUODOSTAMINEN PALVELIMEEN

Nyt voit ottaa SSH-yhteyden palvelimeesi **PuTTY**-yhteysohjelman avulla. Lataa **PuTTY**-yhteyssovellus samalta lataussivulta, kun **PuTTYgen**: PuTTY-lataussivusto
Etsi listasta **PuTTY** ja klikkaa sen jälkeen olevaa linkkiä **”putty.exe”**.

Avaa **PuTTY** ja siirry valikkoon **”Connection > SSH > Auth”** ja lisää **.ppk**-muodossa oleva salausavain klikkaamalla **”Browse”**.

Siirry tämän jälkeen sivulle **”Session”** ja syötä kenttään **”Host Name (or IP address)”** palvelimesi IP-osoite. Varmista, että yhteydenottotavaksi on valittu **”SSH”**. Klikkaa tämän jälkeen **”Open”**.

Sinulle aukeaa seuraavaksi komentorivi, jossa kysytään käyttäjätunnusta. Kirjoita käyttäjätunnukseksi **”centos”** (jos palvelimen käyttöjärjestelmä on Centos. Vaihtoehtoisesti Ubuntu-käyttöjärjestelmissä: **“ubuntu”** ja Debian-käyttöjärjestelmissä **“debian”**) ja klikkaa Enter-painiketta.

Komentorivi kysyy sinulta seuraavaksi salasanaa. Syötä tähän salasana, jonka loit **.ppk**-tiedstoa luodessa ja klikkaa Enter-painiketta.

Olet nyt onnistuneesti ottanut palvelimeesi SSH-yhteyden.

5.3. LINUX/OS X SSH YHTEYDEN MUODOSTAMINEN LINUX PALVELIMEEN

Linux- / OS X-järjestelmissä ei tarvitse PEM-muotoista sertifikaattia konvertoida toiseen muotoon, vaan yhteys voidaan muodostaa PEM-avainta käyttämällä.

Seuraavalla komennolla voidaan muodostaa yhteys. Tunnus on käyttäjätunnus ja IP on palvelimen julkinen IP-osoite.

ssh -i /path/to/pem-file tunnus@ip

6. YHTEYDEN MUODOSTAMINEN (WINDOWS)

Jos haluat ottaa Windows-palvelimeesi yhteyttä esimerkiksi RDP:llä, muistathan ensin sallia palvelimelle RDP-yhteyden. Katso ohjeet tähän kappaleesta **4.4. Security Groupin luominen**.

Siirry pudotusvalikkoon **”Compute”** ja valitse pudotusvalikosta valinta **”Instances”**. Klikkaa palvelinlistauksessa sen palvelimen nimeä, johon olet ottamassa yhteyttä. Siirry tämän jälkeen välilehdelle **”Console”**. Mikäli konsoli ei aukea, klikkaa tekstiä **”Click here to show only console”**.

Ensimmäisen kirjautumisen yhteydessä sinun tulee määrittää salasana palvelimelle. Ennen salasanan määrittämistä konsolin kautta palvelimelle ei voi ottaa yhteyttä muuta kautta.

Kun olet asettanut salasanan, voit ottaa esimerkiksi RDP-yhteyden palvelimelle (Windows-käyttöjärjestelmän Remote Desktop Connection –sovellus).

7. OPENSTACK-DOKUMENTAATIO

http://docs.openstack.org/user-guide/content/